Exhibit D,F,G

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L2 – Service Category 2: Network-Based Asset Discovery

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Armis Centrix

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: A Network-Based Asset Discovery Solutions identifies devices and systems communicating within the network infrastructure without the need for software agents to be deployed to most endpoints or servers. By analyzing network traffic, the Solution should detect all connected assets, including those that do not run traditional operating systems, such as IoT devices, switches, routers, and printers.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Armis Centrix is a completely passive solution that analyzes network traffic to discover and monitor all device types. There are no agents to deploy. A fundamental tenet of Armis is to provide a completely passive collection mechanism to prevent any possibility of causing harm to any sensitive devices, and eliminate the challenges of deploying and managing agents.

Armis Centrix™, the Armis cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time.

Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates security findings and vulnerabilities, and protects your entire attack surface. Armis Centrix™ works in conjunction with your existing security ecosystem and gives organizations peace of mind in knowing that all assets are protected 24/7 by the industry's #1 asset intelligence cybersecurity company.

Armis Centrix™ is deployed at scale in verticals and industries including Manufacturing, Health and Medical, Information Technology, Energy and Utilities, Financial Services, Transportation, Telecommunications and Media, Public Sector and much more.

Our unique out-of-band sensing technology discovers and analyzes all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more.

Key features that make Armis Centrix™ the go to platform for Total Exposure Management:

- Discover all assets for a complete, real-time, always. Accurate inventory.
- Identify and analyze risks such as: vulnerabilities, out-of-date OS and apps, default credentials, invalid certificates or compromised devices.
- Build a risk-reduction program including remediation, enforcement actions and reporting.
- Detects threats and abnormal activity by continuously analyzing the network traffic using multiple methods.
- Stop attacks and minimize their impact. Collect and investigate forensic data to investigate a device's network activity timeline before, during and after an incident.
- Create policies and queries that highlight boundary violations, then automate your segmentation processes with intelligent recommendations.
- Agentless solution which works with all devices, managed and unmanaged.

Why more governments are trusting Armis to deliver better outcomes:

• ROI: address deployment gaps, eliminate unnecessary spendings and technical debt

• Cyber resilience: take well-informed security decisions based on our world-leading real-time asset inventory capabilities

• Reputation and trust: with adherence to various compliance requirements, your organization is seen and trusted as a secure industry leader

Efficiency: focus on high business impact risks that are most likely to be exploited

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Agentless Discovery – Solution should be capable of using passive network scanning techniques that observe traffic and communications, including deep packet inspection (DPI) and flow-based analysis.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Armis Centrix leverages DPI of traffic at layers 4-7 to extract network metadata to help identify devices and show the interaction/communication with other assets. Identification of device behavioral attributes includes applications installed, exploit code delivery, malicious actions, clear text auth, http\s activities, DNS activity, etc.

The aggregated metadata (client and server devices, port, protocol, traffic volume, etc.) is made visible, searchable, and alert-able for flow-based analysis.

Prompt 3: Continuous Network Monitoring – Solution should automatically detect new devices as they are added to the network, whether they are traditional endpoints, virtual machines, or IoT devices.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Centrix provides real time device discovery and asset intelligence for all device types.

When Centrix detects a new device, it uses the information captured about the device's behavior and compares it with 15+ million known device profiles stored in the Armis Asset Intelligence Engine. This comparison allows Centrix to quickly identify and classify devices with a high degree of accuracy including specific information like device make, model, location, and expected behaviors.

Prompt 4: Granular Device Identification – Solution should collect metadata such as MAC address, IP address, operating system, software versions, device make and model and open ports.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Metadata captured:

1. IP address, MAC address, username, device type/category, model, operating system, running applications, etc.

2. wireless MAC layer (WiFi/BlueTooth), protocols used (DNS, HTTPS, VOIP, etc.), amount of data transmitted, encryption, etc.

3. Headers: requests/headers of responses, DHCP packets, etc.

4. TCP/IP handshakes, channel/encryption negotiation, etc.

Leveraging the Asset Intelligence Engine, metadata enables Armis to classify device attributes like device make and model.

Prompt 5: Network Topology Visualization – Solution should map discovered devices and displays how they connect and communicate within the network. The visualization should dynamically update as devices are added, removed, or reconfigured.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

The Armis Centrix Network Mapper tool creates a graphical network and device map of the environment. This map is interactive (drill down, move, etc) and is updated in real time as new devices are discovered, or devices ‘move’ within the environment.

Prompt 6: Customizable Device Grouping and Tagging – Solution should allow administrators to categorize assets based on network segment, physical location, or function (e.g., servers, IoT, printers).

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Armis automatically categorizes a number device attributes - sites, segments, boundaries, location, device category and type, etc.

For more granular or customer categorization, assets in Armis can be “tagged” manually, or automatically via using a policy or through API. Tags can be associated with network segments, physical location, function, owner, or any string determined important by the Centrix User.

Tags can be used in search, dashboards, reports and policies.

Prompt 7: Vulnerable Detection – Solution should identify outdated software versions, unpatched firmware, or insecure configurations that could expose the network to threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Centrix discovers all assets within your environment including the applications (by version) used by a given device.

With these insights, Armis identifies outdated/unpatched software and firmware. Centrix will automatically assign risk factors to a device with outdated software, increase the device risk score, and identify associated CVE's related to the software/firmware version.

Leveraging Armis query language, users can identify devices with old, possibly insecure, versions of an application.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time insights into suspicious network activity, such as communication with known malicious IP addresses or domains. Solution should flag devices that may be compromised or communicating with threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Armis Centrix is able to integrate with third-party threat intelligence solutions/feeds by utilizing its flexible and open architecture. The platform allows for easy integration of APIs and connects with a wide variety of threat intelligence feeds.

This enables Armis Centrix to gather threat intelligence data from multiple sources, including other security solutions, public repositories, and proprietary feeds.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Armis will use commercially reasonable efforts to maintain Uptime Availability of at least 99.9% per month as monitored by Armis' Platform availability monitoring systems.

Armis offers Service Level Objectives for the initial response to Customer support tickets based on the severity of the Customer impact. The ticket priority is based on the business impact as described below:

Armis offers Service Level Objectives for the initial response to Customer support tickets based on the severity of the Customer impact. The ticket priority is based on the business impact as described below:

- Critical (Severity 1) - The Platform is down, all functionalities are not operational and the issue is directly disrupting customer network and/or business operations. No reasonable workaround is available. Support will respond within 1 hour and will work continuously until the issue is fixed.
- High (Severity 2) - A major Platform functionality is impacted by an issue that is persistent and affects many users. No reasonable workaround is available. Support will respond within 8 business hours and will work through the normal business day.
- Medium (Severity 3) - Platform is operational, with a minor impact on functionality for some or all users, and an acceptable workaround or solution exists. Support will respond within 2 business days and will reasonably work through the issue as resources are available.
- Low (Severity 4) - Minor issues not impacting Platform functionality. Support will respond within 4 business days and will reasonably work through the issue as resources are available.

ARMIS PLATFORM TERMS AND CONDITIONS

These Armis Platform Terms and Conditions (these "Terms") are between the Armis entity identified in Section 16.1 below ("Armis") and the customer who purchased the subscription to the Armis Solutions ("Customer"). Armis and Customer may be referred to individually as a "Party" or collectively as the "Parties." Capitalized terms used in these Terms have the meanings assigned to such terms as designated herein. Unless Customer and Armis have signed another agreement which expressly governs Customer's subscription to and use of the Armis Solutions and overrides these Terms, by accepting these Terms via the signing or otherwise indicating acceptance of an applicable Purchase Order, by clicking through to access the Armis Platform, or by otherwise indicating Customer's acceptance of these Terms through access to and/or use of the Armis Solutions (and such date, the Effective Date unless another date is indicated in the Purchase Order as described in Section 4.1), Customer agrees to be bound by these Terms and the person acting on Customer's behalf hereby represents to Armis that they have the authority to bind Customer to these Terms through such consent or access to the Armis Solutions. If Customer does not agree to these Terms or you do not have the authority to bind Customer to these Terms, then Customer may not access to or use the Armis Solutions. The Parties agree as follows:

1. Definitions.

1.1 “Affiliate” means any entity that directly, or indirectly through intermediaries, controls, is controlled by, or is under common control with a Party.

1.2 “Armis APIs” means the Armis’ proprietary application programming interfaces and /or software development kits (SDK) made available to Customer for use in integrating the Armis Platform with other products and applications, in each case solely in accordanceArmis API/SDK License Agreement available here: https://www.armis.com/legal-compliance/.

1.3 “Armis Assets” means: (i) the Armis Solutions and Documentation; (ii) Armis APIs; and (iii) all specifications, technology, software (including all underlying source code and object code), data, methodologies, machine learning models, user interfaces, algorithms, enhancements, components, documentation, techniques, designs, inventions, works of authorship, and know-how, in each case, that are used to provide, or made available in connection with, any of the Armis Solutions , and in each case all associated Intellectual Property Rights, and any subsequent updates, upgrades, and derivatives of any of the foregoing.

1.4 “Armis Platform” means (i) the Armis Software as a Service (SaaS) products (“Armis SaaS”); (ii) Collectors; and (iii) Collector Technology.

1.5 “Armis Solutions” means: (i) the Armis Platform; (ii) Armis APIs; and (iii) Professional Services.

1.6 “Authorized User” means any individual who accesses or uses the Armis Solutions on behalf of Customer or its Affiliates.

1.7 “Collector” means hardware, if any, such as servers or network ports, provided by or on behalf of Armis to Customer to enable the use of the Armis Platform.

1.8 “Collector Technology” means Armis’ virtual machine images or Collector-related software provided by or on behalf of Armis to Customer to enable use of the Armis Platform.

1.9 “Customer Data” means Customer’s data automatically collected, processed, hosted by the Armis Platform through Customer’s use of the Armis Solutions, including copies, modifications, and other derivatives of such data that is generated by the Armis Platform through Customer’s use of the Armis Platform. Customer Data does not include Statistical Data.

1.10 “Documentation” means any technical user guides, manuals, release notes, installation notes, specifications, “read-me” files, support guides, and other materials related to the Armis Solutions, and the use, operation, and maintenance thereof, including all enhancements, modifications, derivative works, and amendments to the same, in each case, that Armis publishes or provides to Customer through its Support Portal available at: https://support.armis.com/s/login (or any successor website, “Support Portal”).

1.11 “Intellectual Property Rights” means all patents, copyrights, moral rights, trademarks, trade secrets, and any other form of intellectual property rights recognized in any jurisdiction, including applications and registrations for any of the foregoing.

1.12 “Laws” means, collectively, any laws, statutes, ordinances, regulations and other types of government authority, promulgated under such authority anywhere in the world.

1.13 “Partner” means an authorized Armis partner, including a reseller, marketplace, or implementation partner.

1.14 “Purchase Order” means: (i) an order form executed by Armis and Customer; or (ii) a purchase order, statement of work, or other similar document issued by Customer or a Partner in each case solely to the extent its terms match and do not deviate from a corresponding Quote. In the event of a conflict between a Purchase Order and a Quote, the Quote will control. If Customer orders Armis Solutions through a Partner or marketplace, then such Partner’s or marketplace’s applicable ordering document will apply solely with respect to the fees payable by Customer, volumes, and subscription term of Armis Solutions ordered.

1.15 “Quote” means a quote prepared and issued by Armis to Customer or a Partner that forms part of these Terms and describes the Armis Solutions ordered by Customer and any associated terms and fees.

1.16 “Professional Services” means any services (beyond the Armis support provided pursuant to Section 2.3.1) such as advisory, consulting, implementation, integration, or training services, that may be provided by or on behalf of Armis to Customer as detailed in an applicable Purchase Order.

1.17 “Statistical Data” means data generated in relation to Customer’s use of the Armis Platform that has been irreversibly anonymized as to Customer and aggregated by Armis. Statistical Data includes generic device descriptions and performance metadata about devices that appear in Customer’s instance of the Armis Platform, such as the device manufacturer, type of operating system, and device model. Statistical Data does not include: (i) any identifiers that would link any devices to Customer, such as IP addresses, MAC addresses, or unique Customer identifiers; or (ii) any data processed on or hosted by any Customer device.

2. Armis Platform.

2.1 Access and Use. During the Subscription Term and subject to Customer’s compliance with these Terms, Armis grants Customer a subscription to access and use the Armis Platform. Customer shall only use the Armis Platform in accordance with the Documentation, solely for Customer’s internal business purposes, and subject to any use limitations indicated in the applicable Purchase Order. The rights granted to Customer herein includes the right to deploy and use the Armis Platform at Customer’s Affiliates’ environments, provided Customer remains fully responsible and liable under these Terms for Customer’s Affiliates’ use. In addition to any access rights a Customer Affiliate may have as aforesaid, a Customer Affiliate may separately subscribe to Armis Solutions pursuant to these Terms by entering into a Purchase Order, and in each case, all references in these Terms to Customer will be deemed to refer to the applicable Affiliate for purposes of that Purchase Order.

2.2 Customer Responsibilities. The Armis Platform may be used by or for Customer only through an account that is specific to Customer and only by Authorized Users. Customer is solely responsible for: (i) identifying and authenticating all Authorized Users, approving access by such Authorized Users to the Armis Platform, and ensuring each Authorized User complies with these Terms; (ii) ensuring that Authorized Users keep their login credentials safe and secure; (iii) all activities that occur under the login credentials of Authorized Users; and (iv) the accuracy, quality, and legality of Customer Data, the means by which Customer acquired Customer Data, Customer's use of Customer Data with the Armis Platform, and the interoperation of any Non-Armis Products with which Customer uses the Armis Platform. Armis is not responsible for any losses or damages arising due to any breach of these Terms by any Authorized User or any other personnel, agent, or advisor of Customer. Customer shall notify Armis immediately upon becoming aware of any unauthorized access to or use of the Armis Platform.

2.3 Provision of the Armis Solutions.

2.3.1 Support. Armis shall provide Customer with standard support (at no additional cost) unless Customer purchases upgraded support as set forth in a Purchase Order. Armis shall provide the technical support and service level commitments set forth in Armis' Platform Support Terms ("SLA"), as updated from time to time, available in the Support Portal. Except for critical updates, Armis schedules maintenance during non-peak usage hours (that reasonably minimizes the impact on all customers worldwide) and shall provide reasonable advance notice through the Armis Platform of any planned downtime in accordance with the SLA.

2.3.2 Updates. Armis makes updates (e.g., bug fixes, enhancements) to the Armis Platform on an ongoing basis, which are delivered through the Armis Platform. Customer's subscription includes all updates that Armis makes generally available to its customers at no additional charge. To the extent Customer's configuration of the Armis Platform requires acceptance of updates, Customer shall accept such updates in a timely manner. Armis is not responsible for the proper performance of the Armis Platform or for any security issues encountered with the Armis Platform resulting from any delay or failure to accept such updates. Armis may update the content, functionality, and user interface of the Armis Platform from time to time, provided that such update will not materially decrease the functionality of the Armis Platform during the Subscription Term. Customer's use of the Armis Solutions under these Terms is not contingent on the delivery of any future features or functionality.

2.3.3 Subcontractors. Armis may utilize subcontractors in the provision of the Armis Solutions, including to process

Customer Data, provided that such subcontractors: (i) are subject to confidentiality obligations materially as protective of Customer Data as those set forth herein; and (ii) maintain commercially reasonable technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Data, taking into account the state of the art, costs of implementation, and the type of data. Armis will be liable for the acts and omissions of its subcontractors to the extent such acts or omissions constitute a breach of these Terms.

2.4 Professional Services. During the Subscription Term, Customer may receive Professional Services subject to these Terms as detailed in a Purchase Order. If applicable, the Armis Quote for Professional Services will identify any additional terms that apply with respect to such Professional Services.

2.5 Data Protection and Security. Armis shall implement and maintain commercially reasonable technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Data, taking into account the state of the art, costs of implementation, and the type of data, in accordance with Armis' information security program, as updated from time to time. Any updates to Armis' information security program will not materially diminish Armis' current data security obligations, a summary of which is available at: https://www.armis.com/legal-compliance/information-security-disclosure/ (or successor website). In addition, the terms and conditions of Armis' Data Processing Addendum ("DPA") found at https://www.armis.com/legal-compliance/data-processing-addendum/ (or successor website), apply to the processing of any Personal Data (as defined in the DPA). Armis shall promptly notify Customer upon becoming aware of a breach the aforementioned security measures within Armis' network leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data ("Security Incident"), and Armis shall reasonably cooperate with Customer in the investigation and mitigation thereof. Armis' obligation to report or respond to a Security Incident is not an acknowledgement by Armis of any fault or liability with respect to such Security Incident. In addition, Armis shall use commercially reasonable efforts to respond, once per year, to any reasonable written inquiries from Customer regarding compliance with this Section 2.5, including requests for Armis' most recent third-party auditor reports regarding Armis' information security program.

2.6 Non-Armis Service Providers. Customer may engage one or more third parties to manage the installation, onboarding, and/or operation of the Armis Platform on Customer's behalf ("Non-Armis Service Provider"), provided that Customer delivers written notice to Armis in advance of such engagement. Customer shall require the Non-Armis Service Provider to comply with these Terms and shall ensure that such Non-Armis Service Provider uses the Armis Platform solely on behalf of Customer. Customer will be fully liable for the acts and omissions of its Non-Armis Service Providers to the extent such acts or omissions constitute a breach of these Terms.

2.7 Non-Armis Products. Customer may from time to time decide to use an integration between Non-Armis Products and the Armis Platform. "Non-Armis Products" means third-party products, applications, services, software, networks, or other systems or information sources acquired by Customer that are not developed by Armis or provided by Armis as part of the Armis Platform. Use of Non-Armis Products is subject to the end user license or other agreement between Customer and the provider of the Non-Armis Products. Armis has no liability with respect to the implementation, maintenance, use, or continued interoperability of any Non-Armis Products, even if Armis designates them as approved or recommended or is an authorized reseller of such Non-Armis Products. By enabling any interoperability between Non-Armis Products and the Armis Platform, Customer expressly agrees to the transfer of any Customer Data between Armis and the provider of the Non-Armis Product as required for such interoperability.

2.8 Restrictions. Customer and its Authorized Users shall not, and shall not authorize any third party to: (i) decompile, disassemble, reverse engineer, copy, frame, or mirror any part of the Armis Assets, or otherwise attempt to derive the source code, structure, ideas, algorithms, or associated know-how of any Armis Assets; (ii) translate, adapt, or modify any Armis Assets; (iii) write or develop any program based upon any Armis Assets, or otherwise access, test, or use any Armis Assets for the purpose of developing or distributing products or services that compete with any Armis Assets; (iv) sell, sublicense, transfer, assign, lease, rent, distribute, grant a security interest in, or otherwise commercially exploit any Armis Assets or make available to a third party any Armis Assets except as expressly authorized in these Terms; (v) use the Armis Assets other than as expressly permitted by these Terms and solely for Customer's internal business operations and in conformity with the Documentation; (vi) alter or remove any trademarks or proprietary notices contained in or on the Armis Assets;

(vii)attempt to gain access to the Armis Platform or its related systems or networks through unauthorized means, including any automated means (i.e., use of scripts or web crawlers), circumvent or interfere with any authentication or security measures of the Armis Platform, or otherwise interfere with or disrupt the integrity or performance of the Armis Platform;

(viii) probe, scan, or test the vulnerability of any Armis system or network; (ix) conduct any competitive analysis, publish or share with any third party any results of any technical evaluation or benchmark tests performed on Armis Assets, or disclose Armis Assets' features, errors, or bugs to a third party without Armis' prior written consent; or (x) use any portion of the Armis Assets in violation of any applicable Laws or transmit to or from the Armis Assets any data, materials, or other content that infringes, misappropriates, or otherwise violates any third-party rights. Customer shall promptly notify Armis in writing if it becomes aware of, or has reason to believe, that any of the prohibitions in this Section have been

breached by Customer, its Affiliates or any Authorized User.

3. Collectors. The Armis Platform may include Collectors that are provided to Customer during the Subscription Term under an applicable Purchase Order. Customer shall use and reasonably maintain Collectors in good working order in accordance with the Documentation and at the locations agreed to by the Parties to enable proper usage and operation of the Armis Platform. Support for Collectors is provided pursuant to Armis' standard support services, as described in the SLA and in the Documentation, which may require installation of a current release of Collector Technology. Without Armis' express written permission, Customer shall not, and shall not permit any third party to: (i) use Collectors other than for the express purpose for which they were provided; (ii) rent or lease Collectors to any third party; (iii) transfer or copy the Collector Technology within the Collector to any other product or device; or (iv) install the Collector Technology on any device other than the applicable Collector for which it was provided. The Armis Platform may not operate as intended if Collectors are moved to any other geographic location without Armis' prior express written permission.

4. Purchase Orders and Fees.

4.1 Subscription Term and Purchase Orders. Each Purchase Order will commence on the subscription start date (the "Effective Date") stated in such Purchase Order and continue until the subscription end date stated therein ("Subscription Term"). Unless otherwise specified in a Purchase Order: (i) subscriptions for the Armis Solutions will automatically renew for additional one (1) year terms unless either Party gives the other written notice (email acceptable) at least thirty (30) days before the end of the relevant Subscription Term; (ii) discounts or other promotional pricing offered for the Armis Solutions are one-time and valid only for the specific amount purchased; (iii) renewal of any discounted Armis Solutions will be at Armis' applicable list price then in effect, and any change in the amount of, or term for, the Armis Solutions may result in re-pricing without regard to prior pricing; and (iv) during a Subscription Term, any purchase of additional amounts will be priced at Armis' applicable list price then in effect.

4.2 Fees. For direct purchases from Armis, Customer shall pay Armis the fees and other amounts detailed in any applicable Purchase Order in accordance with the terms therein. If applicable, Customer shall reimburse Armis for reasonable, documented, out-of-pocket expenses (including all travel costs and expenses) that are authorized by Customer in writing and that are incurred by

Armis in the course of providing Professional Services. If Customer’s use of the Armis Solutions exceeds the usage limitations set forth in the applicable Purchase Order, then Armis may invoice Customer, and Customer shall pay, for such excess usage at Armis’ then current rates, prorated for the remainder of the Subscription Term. Upon renewal, Customer’s subscription will be increased to reflect Customer’s actual usage during the preceding Subscription Term. Armis Solutions purchased cannot be decreased during a Subscription Term.

4.3 Payment Terms. Armis’ obligations under these Terms are conditioned on Customer’s payment in full of the fees when due as set forth in the applicable Purchase Order. For direct purchases from Armis, all fees are billed annually in U.S. Dollars with net thirty (30) payment terms, unless alternate terms are stated in the applicable Purchase Order. Customer shall make any good faith dispute of an invoice in writing within thirty (30) days of the applicable invoice date. If Customer (or a Partner through whom Customer purchased) fails to pay any amounts set forth in a Purchase Order when due, Armis reserves the right to suspend Customer’s access to the Armis Solutions thirty (30) days following Armis’ written notice to Customer of nonpayment until Armis receives payment in full. Any fees not paid when due or not subject to a good faith dispute will accrue interest on a daily basis until paid in full at the lesser of: (i) the rate of one percent (1%) per month; and

(ii) the highest amount permitted by applicable law. Except as expressly stated in these Terms, all fees due or paid are non- cancellable and non-refundable. Neither Party may set-off fees payable under these Terms or a Purchase Order against any other amounts owed to such Party. Customer requirements for purchase orders, vendor registration forms, vendor portals, or the like, will not change Customer’s payment obligations herein.

4.4 Taxes. All amounts payable under these Terms are exclusive of all sales, use, value-added, withholding, and other direct or indirect taxes, charges, levies, and duties, and all such amounts are Customer’s sole responsibility, provided that Customer is not responsible for any taxes on Armis income. These taxes (if applicable) will be stated separately on each invoice, unless Customer provides (in advance) a valid tax exemption certificate authorized by the applicable taxing authority. In addition, if applicable law requires Customer to withhold any amounts on payments owed to Armis pursuant to these Terms, Customer shall: (i) effect such withholding and remit such amounts to the appropriate taxing authorities; and (ii) ensure that, after such deduction or withholding, Armis receives and retains, free from liability for such deduction or withholding, a net amount equal to the amount Armis would have received and retained in the absence of such required deduction or withholding.

5. Beta Products. FROM TIME TO TIME, ARMIS MAY OFFER CUSTOMER THE OPPORTUNITY (WHICH CUSTOMER MAY REFUSE IN ITS SOLE DISCRETION) TO USE EARLY AVAILABILITY OR BETA PRODUCTS, FEATURES, OR DOCUMENTATION (COLLECTIVELY, “BETA PRODUCTS”). BETA PRODUCTS MAY NOT BE GENERALLY AVAILABLE, ARE PROVIDED STRICTLY “AS IS,” AND WILL NOT BE SUBJECT TO ANY REPRESENTATIONS, WARRANTIES, INDEMNIFICATION OBLIGATIONS, OR SUPPORT OBLIGATIONS. UNLESS

PROHIBITED BY LAW, ARMIS WILL HAVE NO LIABILITY RELATED TO SUCH BETA PRODUCTS IN EXCESS OF ONE THOUSAND USD ($1,000.00 USD). CUSTOMER OR ARMIS

MAY TERMINATE CUSTOMER'S ACCESS TO BETA PRODUCTS AT ANY TIME FOR ANY OR NO REASON.

6. Ownership and Reservation of Rights.

6.1 Armis. Except for the rights expressly granted to Customer in Section 2.1, as between the Parties, Armis and/or its licensors own and retain all rights, title, and interest, including Intellectual Property Rights, in and to all Armis Assets, Armis Confidential Information, and any other tangible and intangible material and information incorporated into or constituting any portion of the Armis Assets (excluding any Customer Data and Customer Confidential Information).

6.2 Customer. Except for the rights expressly granted to Armis in this Section 6, as between the Parties, Customer owns and retains all rights, title, and interest in and to Customer Data, Customer Confidential Information, and Feedback, including all associated Intellectual Property Rights. During the Subscription Term, Customer shall provide to Armis the right to access, process, transmit, store, use, and disclose Customer Data as necessary to provide the Armis Solutions to Customer and to improve the Armis Solutions including to identify, investigate, or resolve technical problems with the Armis Solutions.

6.3 Feedback. Customer or an Authorized User may provide to Armis, directly or indirectly, feedback, analysis, suggestions, or comments about the Armis Assets or Armis Solutions (collectively, "Feedback"). Feedback does not include Customer Data or Customer Confidential Information. Customer hereby grants to Armis a non-exclusive, perpetual, irrevocable, transferable, royalty-free, and worldwide right, with the right to grant and authorize sublicenses, to use and benefit from such Feedback to provide and improve the Armis Assets and Armis' business without any compensation or credit due to Customer.

6.4 Statistical Data. During the Subscription Term, Armis may collect and compile Statistical Data and Armis owns and retains all rights, title, and interest in such Statistical Data. Armis may use Statistical Data for its own business purposes (such as improving, testing, and maintaining the Armis Solutions, including training Armis' machine learning algorithms and artificial intelligence models associated with the Armis Solutions, identifying trends, and developing additional products and services).

6.5 Reservation of Rights. Each Party retains all rights that are not expressly licensed to the other Party in these Terms and does not grant the other Party any implied licenses in these Terms or under any other theory.

7. Confidentiality.

7.1 "Confidential Information" means any non-public information disclosed in any form or manner by one Party ("Discloser") to the other Party ("Recipient") that is marked as "confidential" or that Recipient knows or reasonably should know is confidential information of Discloser given the nature of such information and the circumstances of its disclosure. Confidential Information of Armis includes the Documentation, auditor reports, security test results and reports, and all communications related to updates to the Armis Assets. Confidential Information does not include Customer Data automatically uploaded to, processed and hosted by the Armis Platform (the security and protection of which is governed by section 2.5), or any information which Recipient can demonstrate through reasonable evidence: (i) is or becomes generally known and available to the public through no act of Recipient; (ii) was already in Recipient's possession without a duty of confidentiality owed to Discloser at the time of receipt; (iii) is lawfully obtained by Recipient from a third party who has the express right to make such disclosure; or (iv) is independently developed by Recipient without breach of an obligation owed to Discloser.

7.2 During the Subscription Term, Recipient may use Discloser's Confidential Information solely for the purpose of performing its obligations under these Terms. Recipient shall use the same degree of care in protecting Discloser's Confidential Information as Recipient uses to protect its own Confidential Information from unauthorized use or disclosure, but in no event less than reasonable care. Recipient shall not disclose Discloser's Confidential Information to any third party except to its employees, consultants, affiliates, agents, and subcontractors having a need to know such Confidential Information to perform their respective obligations under these Terms and who are bound by a written undertaking of confidentiality that is at least as protective of Discloser's Confidential Information as set forth herein. In addition, Recipient may disclose Discloser's Confidential Information to the extent such disclosure is required by law or order of a court or similar judicial or administrative body, provided that Recipient notifies Discloser in advance (unless legally prohibited from doing so) to enable Discloser to seek a protective order or otherwise seek to prevent or restrict such disclosure. All right, title, and interest in and to Confidential Information is and will remain the sole and exclusive property of Discloser. Recipient is solely responsible and liable to Discloser for any act, omission, or other failure to comply with the terms of the Agreement by any of its Representatives.

7.3 The use and disclosure restrictions in this Section 7 (Confidentiality) will survive the expiration or termination of these Terms for a period of three (3) years, provided that Confidential Information defined as a trade secret under any applicable

Laws shall be maintained by Recipient in confidence so long as it retains trade secret status under such Laws.

8. Warranties.

8.1 Armis Warranties.

8.1.1 Armis Platform Warranties. Armis warrants that: (i) during the Subscription Term, the current versions of the Armis Platform will perform and function materially in accordance with the Documentation under normal and authorized use in compliance with these Terms; and (ii) Armis shall maintain appropriate technical measures and periodically update the Armis Platform to prevent the introduction of software viruses, disabling devices, trojans, worms, or other software or hardware devices designed to intentionally disrupt, disable, or harm Customer's network or systems or the operation of the Armis Platform. If Customer believes the Armis Platform does not conform to the warranties in this Section 8.1.1, Customer shall promptly notify Armis in writing (in no event later than thirty (30) days from the date of discovery of the nonconformity) by submitting a support ticket via the Support Portal in accordance with the SLA. In the event of a breach of the warranties in this Section 8.1.1, Armis' exclusive responsibility, and Customer's exclusive remedy (other than any termination rights Customer may have under Section 14), will be for Armis to either correct or replace, at no additional charge to Customer, the applicable deficiency in the Armis Platform in accordance with the SLA.

8.1.2 Professional Services Warranty. Armis warrants that, during the Subscription Term, the Professional Services will be performed in a workmanlike manner in accordance with current industry standards. If Customer believes the Professional Services do not conform to the warranty in this Section 8.1.2, Customer shall promptly notify Armis in writing (in no event later than thirty (30) days from the date the Professional Services were performed) by submitting a support ticket via the Support Portal in accordance with the SLA. Armis' exclusive responsibility, and Customer's exclusive remedy, will be for Armis, at its option and expense to: (i) re-perform the applicable Professional Services that fail to meet this warranty; or (ii) issue a refund of the fees paid for the applicable non-conforming Professional Services.

8.1.3 Exceptions. The warranties set forth in this Section 8.1 will not apply to the extent the nonconformity results from or is otherwise attributable to any failure or damage caused by the actions or inactions of Customer, Authorized Users, or any person acting at Customer's direction.

8.2 Customer Warranty. Customer warrants it will have all rights necessary, including any required consents, to provide or make available to Armis the Customer Data (including personal data) or other materials in connection with its use of the Armis Solutions and to permit Armis to use Customer Data pursuant to these Terms.

9. Mutual Representations. Each Party represents that: (i) it is duly organized, validly existing and in good standing under the Laws of its jurisdiction of incorporation or organization; (ii) it has the full corporate power and authority to execute, deliver, and perform its obligations under these Terms; (iii) the person signing or clicking through these Terms on its behalf has been duly authorized and empowered to enter into these Terms; and (iv) these Terms are valid, binding, and enforceable against it in accordance with its terms.

10. Compliance with Laws. In connection with the performance of these Terms, each Party shall comply with all Laws applicable to such Party in the conduct of its business generally. In addition, if Customer's use of the Armis Solutions requires Customer to comply with industry specific Laws applicable to such use, Customer is responsible for such compliance. Customer shall not use, export, re-export, ship, or transfer the Armis Platform to any country subject to an embargo or comprehensive sanction by the U.S., EU, UN Security Council, or other applicable jurisdiction ("Embargoed Country"), or to a person or entity subje

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L2 – Service Category 2: Network-Based Asset Discovery

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Palo Alto Networks NGFW IoT Cloud-Delivered Security

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7)
  = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: A Network-Based Asset Discovery Solutions identifies devices and systems communicating within the network infrastructure without the need for software agents to be deployed to most endpoints or servers. By analyzing network traffic, the Solution should detect all connected assets, including those that do not run traditional operating systems, such as IoT devices, switches, routers, and printers.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Palo Alto Networks' IoT solution leverages advanced machine learning (ML) and artificial intelligence (AI) to provide comprehensive visibility into all connected assets, including IoT devices, switches, routers, printers, and more. The IoT solution continuously monitors network traffic patterns to identify devices based on their unique communication behaviors. By analyzing data packets and communication protocols, the system can determine the type and role of each device, even if it doesn't run a standard OS. The solution employs ML algorithms that compare detected device behavior with extensive threat intelligence and device profile databases. This approach allows the solution to accurately classify assets without relying on traditional endpoint agents or signatures. Palo Alto Networks' solution uses passive monitoring to detect devices in real time as they connect to the network. The solution is designed to work in environments that include IoT and OT devices, such as industrial sensors, smart printers, and building management systems. These devices often use proprietary or specialized communication protocols that the solution can recognize, enabling it to discover assets that traditional monitoring tools may miss.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Agentless Discovery – Solution should be capable of using passive network scanning techniques that observe traffic and communications, including deep packet inspection (DPI) and flow-based analysis.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Palo Alto Networks' IoT solution leverages passive network scanning techniques—specifically DPI and flow-based analysis—to gain comprehensive visibility and insight into IoT devices and their traffic. This combination ensures non-intrusive, real-time monitoring and enhanced security for all connected assets in the network.

Prompt 3: Continuous Network Monitoring – Solution should automatically detect new devices as they are added to the network, whether they are traditional endpoints, virtual machines, or IoT devices.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Palo Alto Networks' IoT solution detects new devices by leveraging advanced network monitoring techniques that provide continuous visibility into network traffic. This approach enables the detection and classification of new devices as they connect to the network, even those that do not support traditional endpoint agents.

Prompt 4: Granular Device Identification – Solution should collect metadata such as MAC address, IP address, operating system, software versions, device make and model and open ports.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Our IoT solution collects metadata such as MAC addresses, IP addresses, operating systems, software versions, device make and model, and open ports through passive monitoring, DPI, flow-based analysis, and protocol-specific dissection. The solution uses machine learning algorithms to analyze the data collected from both DPI and flow-based analysis. These algorithms compare the new device's traffic and behavior against a comprehensive database of known device profiles.

Prompt 5: Network Topology Visualization – Solution should map discovered devices and displays how they connect and communicate within the network. The visualization should dynamically update as devices are added, removed, or reconfigured.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Palo Alto Networks IoT solution maps discovered devices and displays how they connect and communicate within the network through real-time, interactive visualizations. This provides administrators with a clear view of their network topology, device interactions, and potential security risks, enabling better-informed decisions for network management and threat prevention. The visualization is updated in real-time, ensuring that changes in the network are reflected.

Prompt 6: Customizable Device Grouping and Tagging – Solution should allow administrators to categorize assets based on network segment, physical location, or function (e.g., servers, IoT, printers).

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Our IoT solution allows administrators to create custom groups based on device type, function, location, etc. Administrators can apply security policies to specific tagged groups, ensuring consistent protection tailored to different device categories. Custom tagging enables better identification and contextual awareness and can be based on attributes like operating system or connected applications, providing a more granular way to manage and filter devices.

Prompt 7: Vulnerable Detection – Solution should identify outdated software versions, unpatched firmware, or insecure configurations that could expose the network to threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The IoT solution integrates with vulnerability databases and threat intelligence feeds, including known vulnerabilities or CVEs associated with specific devices, operating systems, or software versions. Metadata collected from device profiling is cross-referenced with these databases to identify any known vulnerabilities relevant to connected IoT devices. The solution provides actionable insights for mitigating vulnerabilities, eg: firmware or configuration updates.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time insights into suspicious network activity, such as communication with known malicious IP addresses or domains. Solution should flag devices that may be compromised or communicating with threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Our IoT solution integrates with threat intelligence feeds, which provide up-to-date information about known device types, vulnerabilities, and potential threats; helping to identify whether a newly detected device matches any known patterns or poses a security risk. The threat intelligence integration enables the solution to detect and respond to new types of devices or protocols as they emerge, providing protection against novel and previously known devices.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SERVICE LEVEL AGREEMENT

IoT Security Service

For its IoT Security service ("Service"), Palo Alto Networks commits to using commercially reasonable efforts to achieve certain service metrics described below. In the unlikely event that Palo Alto Networks does not meet these commitments, Customers will be eligible to receive a service credit.

1. Definitions

1.1 "Available" means that the Service is capable of processing and presenting Customer's data in accordance with Service documentation.

1.2 "Available Time," in minutes, is when the Service is Available during a calendar month.

1.3 "Total Time" is the total number of minutes in a calendar month.

1.4 "Excluded Time" means the time, in minutes, described in the section entitled "Exclusions" below.

1.5 "Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during a given rolling six-month period during which the Service was not Available. The Uptime Percentage measurements exclude Exclusions. It is formulated as,

uptime percentage = available time / (total time - excluded time)

2. Service Level Commitments

Palo Alto Networks will use commercially reasonable efforts to make the Service Available with an Uptime Percentage of at least 99% during any given rolling six-month period ("Service Level"). In the event that the Service does not meet the Service Level, Customer will be eligible to request a Service credit. Service credits are calculated as a percentage of the total charges paid by Customer for the monthly billing cycle in which the Service fell below the Service Level.

Uptime Percentage	Service Credit
Less than 99% but equal to or greater than 98%	5%
Less than 98%	10%

3. Exclusions

Customer agrees and acknowledges that the IoT Security service is a tool that monitors network traffic used by certain IoT devices and is not capable of detecting intrusions or other security issues outside the normal parameters defined by Palo Alto Networks in the Service

documentation. Palo Alto Networks will attempt to monitor as much network activity as possible, but it may not be possible to monitor certain devices that are obscured behind a different intranet environment such as a layered network address table or other obstacle to intranet TCP/IP communication. Network latency and throughput may also affect the responsiveness of the Service. Palo Alto Networks is unable to monitor network traffic that is encrypted, encapsulated, tunneled, compressed or otherwise obfuscated. This Service Level Agreement shall not apply and the Service shall be deemed Available where the loss of Service results from:

(i) Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

(ii) Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;

(iii) Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties including, but not limited to, force majeure events;

(iv) Any actions or inactions of Customer or any third party, including failure to assist in Palo Alto Networks' efforts to provide support;

(v) Planned and unplanned maintenance windows;

(vi) High Availability events and scaling events;

(vii) Fetching of logs from Cortex Data Lake service;

(viii) Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Agreement (www.paloaltonetworks.com/legal/eula).

4. Administration

4.1 Customer may, at any time, obtain Service status here (https://status.paloaltonetworks.com).

4.2 To qualify to receive Service credit under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to beta, trials and evaluations of the Service provided at no cost to the Customer.

4.3. Customer must submit a claim by opening a ticket on the Palo Alto Networks Customer Support Portal. To be eligible, the credit request must be received by Palo Alto Networks within 24 hours of an outage or an incident. Customer's failure to request and to respond to other information as required will disqualify Customer from receiving a Service credit.

4.4 When the claim is confirmed by Palo Alto Networks to be less than the Service Level, then Palo Alto Networks will issue a service credit by applying it against future Service payments due from Customer. Service credits will not entitle Customer to any refund or other payment from Palo Alto Networks.

4.5 If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the service credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer.

4.6 The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of breach of this Service Level Agreement.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term "Product" is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS "CUSTOMER", "END USER", "YOU" or "YOUR") AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS "PALO ALTO NETWORKS").

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

"Affiliate" means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where "Control" means having the power, directly

or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks' use of all Palo Alto Networks Affiliates to deliver Products and Services.

"End User Data" means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

"Enterprise Program" means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

"Hardware" means hardware-based products listed on Palo Alto Networks' then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

"Product" means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

"Published Specifications" mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. "Software" means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

"Subscription(s)" means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

"Systems Data" means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be

subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices

or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED “AS IS”. PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks’ suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks’ suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer’s payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party’s patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a “Claim”), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the

defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and

communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include

Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L2 – Service Category 2: Network-Based Asset Discovery

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Tenable Vulnerability Management

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: A Network-Based Asset Discovery Solutions identifies devices and systems communicating within the network infrastructure without the need for software agents to be deployed to most endpoints or servers. By analyzing network traffic, the Solution should detect all connected assets, including those that do not run traditional operating systems, such as IoT devices, switches, routers, and printers.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Tenable Vulnerability Management supports the discovery of assets without scanning the assets for vulnerabilities. Tenable can detect anything with an IP.

Tenable provides scan templates for discovery scanning and passive detection using Tenable Nessus Network Monitor in discovery mode. Tenable Vulnerability Management also supports connectors from third parties such as ServiceNow or API calls to manually enter the assets. Assets that have not been scanned for vulnerabilities do not count towards the organization's asset license limit. After assets are discovered in this manner, a strategy can be developed to categorize and scan assets for vulnerabilities.

Tenable Vulnerability Management supports unlimited discovery scans using both active and passive sensors. Customers can use these scans to comprehensively inventory all of their assets and determine the appropriate license size. Tenable scans in an unlimited manner. Tenable customers are currently scanning millions of assets. The elastic nature of our cloud infrastructure allows for unlimited scanning. In the customer environment, scaling can be handled by:

Deploy an unlimited number of Nessus Scanners. Tenable recommends at least one scanner in each firewall zone to prevent interference of scan results by the firewall. Depending on the customer environment, it may be ideal to deploy Nessus Scanners on each network segment. Nessus Scanners on local network segments can detect systems via ARP pings that would normally not be detected by scanners on other network segments.

Multiple Nessus Scanners can be deployed to handle large scans by load-balancing the work across the scanners. This can also be useful for completing smaller scans in a very short time frame.

Deploying Nessus Scanners at multiple geographic locations allows scans to be done without consuming WAN bandwidth.

Deploy an unlimited number of Nessus Agents. Nessus Agents allow the scanning of large amounts of endpoints in a very short period since all the agents scan in parallel. Optional agent deployments can be useful in remote locations where the customer does not want to deploy a Nessus Scanner.

Tenable's Host Discovery scans can be run on an unlimited number of IP addresses and there will be no license count incurred. The Host Discovery scans only use plugins that are not counted towards the license. To identify live hosts in the scan settings, you can set to Ping the remote host, if set to on, the scanner pings remote hosts on multiple ports to determine if they are alive.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Agentless Discovery – Solution should be capable of using passive network scanning techniques that observe traffic and communications, including deep packet inspection (DPI) and flow-based analysis.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes, agentless discovery is done via passive scanning through the Nessus Network Monitor , which can can passively monitor network traffic and communications. Using techniques like deep packet inspection (DPI) and flow-based analysis, it identifies devices across the network without deploying agents. This ensures continuous, non-intrusive visibility of all connected assets, including IoT, unmanaged devices, enhancing monitoring without impacting performance.

Prompt 3: Continuous Network Monitoring – Solution should automatically detect new devices as they are added to the network, whether they are traditional endpoints, virtual machines, or IoT devices.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes, solution can automatically detect new devices added to the network, including traditional endpoints, virtual machines, and IoT devices. This is achieved through host discovery scans from a Nessus Scanner or passive scanning. The Nessus Network Monitor provides continuous monitoring without actively targeting devices, which is ideal for fragile or sensitive devices. It can also automatically launch scans against new devices discovered by our Passive Sensor.

Prompt 4: Granular Device Identification – Solution should collect metadata such as MAC address, IP address, operating system, software versions, device make and model and open ports.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Tenable's products can scan anything with an IP. The products can detect the common software that runs on these devices. Tenable takes a true asset-centric approach to vulnerability scanning and collects metadata about assets, including IP addresses, URLs, FQDNs, NetBIOS names, MAC addresses, BIOS UUIDs, Docker Image IDs, and more. Host Discovery scans can be run on an unlimited number of IP addresses and there will be no license count incurred.

Prompt 5: Network Topology Visualization – Solution should map discovered devices and displays how they connect and communicate within the network. The visualization should dynamically update as devices are added, removed, or reconfigured.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

No - Tenable Vulnerability Management does not provide mapping of assets in a network topology technology format. However, our products aggregate vulnerability scan data from Nessus scanners, agents, and Nessus Network Monitor devices. The results can be imported into most (market leading) Network Topology & Risk Analysis tools. For a full list of integration partners, please visit: https://www.tenable.com/partners/technology

Prompt 6: Customizable Device Grouping and Tagging – Solution should allow administrators to categorize assets based on network segment, physical location, or function (e.g., servers, IoT, printers).

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Tenable supports the creation, modification, & customization of asset tags. Assets can be tagged manually or dynamically. Tags can be used to searchs & filtered by tags. Tags can then be used as scan targets & as filters of dashboards. These groupings are customizable on many technical delimiters such as; OS, Software installed, ports found open, device behavior, infrastructure technologies, vulnerabilities found, & complicated attribute combinations.

Prompt 7: Vulnerable Detection – Solution should identify outdated software versions, unpatched firmware, or insecure configurations that could expose the network to threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Yes, core product feature. Our solution can scan anything with an IP & detect certain information depending on the device type. All major device types are supported via active scanning as well as configuration assessments. Tenable plugins will run checks on the assets & identify individual vulnerabilities, including when the vulnerability was first discovered & the current age of the individual vulnerabilities.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time insights into suspicious network activity, such as communication with known malicious IP addresses or domains. Solution should flag devices that may be compromised or communicating with threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Asset categorization is done in real time via manual or automatic tag. When assets are discovered & identified, the tool automatically assigns tags to categorize them based on these attributes. These tags allow for easy organization & management of assets within the network.

Additionally, Tenable's Vulnerability Intelligence offers deep insights & detailed timelines for informed decisions & accelerated incident response.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SLA: Uptime Guarantee: https://static.tenable.com/prod_docs/Service_Level_Agreement.pdf

Master Agreement, accepted via a click-thru acknowledgement at time of installation: https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L3 – Service Category 3: Endpoint Detection and Response

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Cortex XDR

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 9. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 9 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 9 are worth a maximum of 4 points total. An individual Evaluator's technical score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-9 / 8) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: An Endpoint Detection and Response (EDR) Solution is designed to provide continuous and comprehensive monitoring of endpoint activities to detect, investigate, and respond to threats in real-time. The Solution collects and analyzes detailed telemetry data, such as file access patterns, process execution, network connections, and registry changes, to identify malicious behavior that traditional antivirus software might miss.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XDR takes a more efficient and practical approach to preventing attacks that eliminates the need for traditional antivirus. Rather than trying to keep up with the ever-growing list of known threats, Cortex XDR sets up a series of roadblocks—also referred to as traps—that prevent attacks at their initial entry points, the points where legitimate executable files might unknowingly allow malicious access to the system. Additionally, Cortex XSIAM comes with Cortex XDR agents as part of the platform. Cortex XDR accurately detects threats through behavioral analytics and reveals root causes to expedite investigations. Tight integration with enforcement points accelerates containment, enabling security teams to stop attacks before significant damage can occur. This comprehensive and integrated approach ensures robust threat prevention and response, significantly enhancing an organization's overall security posture.

● Proven endpoint protection: Block advanced malware, exploits and fileless attacks with the industry's most comprehensive endpoint security stack. Our lightweight agent stops threats with Behavioral Threat Protection, AI and cloud-based analysis.

● Laser accurate detection: Pinpoint evasive threats with patented behavioral analytics. Cortex XDR uses machine learning to profile behavior and detect anomalies indicative of attack. Analytics lets you spot adversaries attempting to blend in with legitimate users.

● Lightning fast investigation and response: Investigate threats quickly by getting a complete picture of each attack with incident management. You can view the root cause of any alert with a single click and swiftly stop attacks across your environment.

Cortex XDR provides:

● Complete Endpoint Security: Safeguard your endpoints with NGAV, host firewall, disk encryption and USB device control.

● ML-Driven Threat Detection: Find hidden threats like insider abuse, credential attacks, malware and exfiltration using behavioral analytics.

● Incident Management: Cut investigation time with intelligent alert grouping. Incident scoring lets you focus on the threats that matter.

● Automated Root Cause Analysis: Swiftly verify threats by reviewing the root cause, sequence of events, intelligence and investigative details all in one place.

● Deep Forensics: Conduct deep internal and regulatory investigations, even if endpoints are not connected to the network.

● Flexible Response: Block fast-moving attacks, isolate endpoints, execute scripts and sweep across your entire environment to contain threats in real time.

● Extended Threat Hunting: Conduct more granular and advanced threat hunting operations in your security environment using extended data collection and analysis.

For more information, please see:

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Documentation

https://www.paloaltonetworks.com/resources/whitepapers/cortex-xdr

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on how the Solution meets the identified technical capabilities and features.

Prompt 2: Real-Time Monitoring and Logging – Solution should provide real-time monitoring and logging of all endpoint activities, including, but not limited to, file changes, process creation and termination, registry edits, network connections, and USB device insertion.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

XSIAM provides real-time monitoring & logging of endpoint activities, file changes, process creation, registry edits, network connections, and USB device insertions. Advanced behavioral analytics, ML, and AI - XSIAM detects anomalies and threats. Integration with other security tools enhances threat correlation, while real-time alerts ensure prompt incident response. Centralized logging and automated response actions facilitate quick threat containment and compliance.

Prompt 3: Behavioral Analytics – Solution should use an extended portfolio of security tools, like endpoint firewalls, device and application control, application inventory, signature matching, vulnerability and patch management and others, plus network-level tools such as secure email and sandboxing.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

XSIAM uses endpoint FWs, device control, application control, device inventory, signature matching, & vulnerability management to detect anomalies and suspicious activities. WildFire, our cloud-based sandboxing engine, detonates unknown files in real time for verdicts, enabling adv. threat detection & response. For email security, protections include SASE native-CASB's email DLP module & XSOAR phishing playbooks, preventing data loss with ML and regex-based patterns.

Prompt 4: Automated Response Mechanisms – Solution should take predefined actions when threats are detected, such as isolating the affected device from the network, terminating malicious processes, or blocking IP addresses.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XDR offers automated response actions to help security teams mitigate threats in real time. Actions include isolating endpoints, stopping malicious processes, rolling back system changes, blocking file execution, disabling network connections, and sending alerts. Cortex XSIAM is enhanced by full SOAR functions, enabling automated responses through customizable playbooks. This ensures threat mitigation, reduces response time and improves security posture.

Prompt 5: Threat Hunting Tools – Solution should allow analysts to query across the entire organization's endpoints, searching for specific indications or compromise (IoCs) or patterns that may indicate the presence of advanced threats.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XDR is a threat hunting tool, allowing analysts to query organization-wide endpoints using XQL. Analysts can search for IoCs or patterns indicating advanced threats. The solution provides comprehensive visibility by deploying agents on endpoints for detailed queries and investigations. Included in Cortex XSIAM, this capability enhances proactive threat detection and overall security posture through complex searches and endpoint data analysis.

Prompt 6: Support for Remote Endpoints – Solution should ensure that devices outside of the network, such as remote or mobile works, are protected and monitored regardless of location.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XDR supports remote endpoints, including telework and geographically distributed teams. Remote endpoints are continuously monitored to understand normal behavior and alert deviations. XDR provides remote device visibility and contextual awareness, even when the device is not on a corporate network.

Prompt 7: Remediation Playbooks – Solution should provide detailed guidance for resolving detected incidents, including step-by-step instructions for isolating infected devices, rolling back malicious changes, and restoring systems to a known good state.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM empowers security teams with its AI-powered Co-Pilot, offering guidance and recommendations for incident response. Its comprehensive SOAR capabilities, including over 1,000 pre-built playbooks and extensive integrations, automate incident response, minimizing manual effort. XSIAM seamlessly integrates with Cortex XDR to enable end-to-end automated remediation.

Prompt 8: Integration of CTI Data Feeds – Solution should provide real-time updates on emerging malware strains, threat actor campaigns, and new attack vectors targeting endpoints. The EDR Solution can use CTI feeds to compare endpoint behavior when known IoCs, enhancing detection and automated response capabilities.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Cortex XDR integrates with VirusTotal to enhance threat detection, investigation, and remediation capabilities. Full CTI data feed ingestion is done through Cortex XSOAR's TIM module, enhancing Cortex XDR's ability to detect and automate the identification of threats based on high-confidence threat intelligence.

Prompt 9: Forensic Capabilities – Solution should allow security analysts to investigate historical endpoint activities, enabling root cause analysis and providing a detailed timeline of events leading up to a security incident.

Cortex XDR meets this requirement with its forensics module, providing robust endpoint logging capabilities. It collects detailed forensic data such as process execution logs, file system changes, network connections, registry modifications, user activities, and USB device interactions. This data gives security teams a complete picture of system activities during an attack or incident, enabling thorough investigation and response.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SERVICE LEVEL AGREEMENT

IoT Security Service

For its IoT Security service (“Service”), Palo Alto Networks commits to using commercially reasonable efforts to achieve certain service metrics described below. In the unlikely event that Palo Alto Networks does not meet these commitments, Customers will be eligible to receive a service credit.

1. Definitions

1.1 “Available” means that the Service is capable of processing and presenting Customer’s data in accordance with Service documentation.

1.2 “Available Time,” in minutes, is when the Service is Available during a calendar month.

1.3 “Total Time” is the total number of minutes in a calendar month.

1.4 “Excluded Time” means the time, in minutes, described in the section entitled “Exclusions” below.

1.5 “Uptime Percentage” is calculated by subtracting from 100% the percentage of minutes during a given rolling six-month period during which the Service was not Available. The Uptime Percentage measurements exclude Exclusions. It is formulated as,

uptime percentage = available time / (total time - excluded time)

2. Service Level Commitments

Palo Alto Networks will use commercially reasonable efforts to make the Service Available with an Uptime Percentage of at least 99% during any given rolling six-month period (“Service Level”). In the event that the Service does not meet the Service Level, Customer will be eligible to request a Service credit. Service credits are calculated as a percentage of the total charges paid by Customer for the monthly billing cycle in which the Service fell below the Service Level.

Uptime Percentage	Service Credit
Less than 99% but equal to or greater than 98%	5%
Less than 98%	10%

3. Exclusions

Customer agrees and acknowledges that the IoT Security service is a tool that monitors network traffic used by certain IoT devices and is not capable of detecting intrusions or other security issues outside the normal parameters defined by Palo Alto Networks in the Service

documentation. Palo Alto Networks will attempt to monitor as much network activity as possible, but it may not be possible to monitor certain devices that are obscured behind a different intranet environment such as a layered network address table or other obstacle to intranet TCP/IP communication. Network latency and throughput may also affect the responsiveness of the Service. Palo Alto Networks is unable to monitor network traffic that is encrypted, encapsulated, tunneled, compressed or otherwise obfuscated. This Service Level Agreement shall not apply and the Service shall be deemed Available where the loss of Service results from:

(i) Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

(ii) Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;

(iii) Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties including, but not limited to, force majeure events;

(iv) Any actions or inactions of Customer or any third party, including failure to assist in Palo Alto Networks' efforts to provide support;

(v) Planned and unplanned maintenance windows;

(vi) High Availability events and scaling events;

(vii) Fetching of logs from Cortex Data Lake service;

(viii) Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Agreement (www.paloaltonetworks.com/legal/eula).

4. Administration

4.1 Customer may, at any time, obtain Service status here (https://status.paloaltonetworks.com).

4.2 To qualify to receive Service credit under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to beta, trials and evaluations of the Service provided at no cost to the Customer.

4.3. Customer must submit a claim by opening a ticket on the Palo Alto Networks Customer Support Portal. To be eligible, the credit request must be received by Palo Alto Networks within 24 hours of an outage or an incident. Customer's failure to request and to respond to other information as required will disqualify Customer from receiving a Service credit.

4.4 When the claim is confirmed by Palo Alto Networks to be less than the Service Level, then Palo Alto Networks will issue a service credit by applying it against future Service payments due from Customer. Service credits will not entitle Customer to any refund or other payment from Palo Alto Networks.

4.5 If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the service credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer.

4.6 The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of breach of this Service Level Agreement.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term "Product" is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS "CUSTOMER", "END USER", "YOU" or "YOUR") AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS "PALO ALTO NETWORKS").

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

"Affiliate" means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where "Control" means having the power, directly

or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks' use of all Palo Alto Networks Affiliates to deliver Products and Services.

"End User Data" means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

"Enterprise Program" means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

"Hardware" means hardware-based products listed on Palo Alto Networks' then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

"Product" means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

"Published Specifications" mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. "Software" means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

"Subscription(s)" means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

"Systems Data" means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be

subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices

or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED “AS IS”. PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks’ suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks’ suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer’s payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party’s patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a “Claim”), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the

defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and

communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include

Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L4 – Service Category 4: External-Facing Asset Discovery

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Cortex Xpanse

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Total Solution Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: External-Facing Asset Discovery Solutions must help organizations identify and assess the security of their publicly accessible digital assets, such as web servers, cloud services, applications, and other internet-facing systems. The Solution must continuously scan the organization's external IP ranges and domains to identify assets that are exposed to the internet and assess their vulnerabilities.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Palo Alto Networks Cortex Xpanse is a comprehensive Attack Surface Management (ASM) platform that continuously scans the entire Internet to help organizations understand their publicly visible footprint. Cortex Xpanse, a component of XSIAM, serves as a comprehensive Attack Surface Management (ASM) tool that will scan most public addresses every 1-2 days and scans all Internet addresses every 2 weeks. Xpanse helps helps organizations manage and mitigate cyber attack risks through:

● Attack surface management: Identify, learn about, and respond to unknown risks in connected systems and exposed services

● Asset discovery: Automatically discovers, monitors, and tracks Internet assets

● Cloud management: Helps organizations manage the unmanaged cloud

● Shadow IT discovery: uncover assets and services that are publicly exposed but not known to IT or security teams.

● Vulnerability Remediation: Assist with prioritizing exposed vulnerabilities to ensure they are not exploited.

● 3rd party support: integrate with SIEM and SOAR platforms to automate responses and streamline remediation processes.

Cortex Xpanse provides an inventory of all internet-facing assets, which can be used to evaluate supplier risk, assess the security of acquired companies, and reduce mean time to detection and remediation. Cortex Xpanse was developed for the Department of Defense and gathers data from a variety of sources, including DNS records, domain registrars, and business registration databases.

By leveraging continuous scanning and advanced analytics, Cortex Xpanse helps security teams proactively manage their external-facing infrastructure, reducing the risk of cyberattacks. It is especially useful for identifying assets that might be exposed unintentionally, such as misconfigured cloud environments, unused domains, and forgotten servers.

For more information, please see:

https://docs-cortex.paloaltonetworks.com/r/Cortex-XPANSE/2/Cortex-Xpanse-Expander-User-Guide/What-is-Cortex-Xpanse

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Contiuous Scanning – Solution should provide continuous scanning of public IP addresses and domains associated with the organization, identifying all internet-facing services, applications, and network devices.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex Xpanse continuously scans the Internet, attributing assets and domains to the organization and enumerating internet-facing services, applications, and devices. Cortex XSIAM scans most public addresses every 1-2 days and all Internet addresses every two weeks. This provides critical insights into potential risks, evaluates supplier risk, assesses acquired companies' security, and reduces mean time to detection and remediation, enhancing overall security posture.

Prompt 3: Service Detection and Banner Grabbing – Solution should collect information such as service versions, SSL/TLS certificate details, and software configurations for each exposed asset.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex Xpanse now includes detailed CVE data, additional service classification, and geolocation information. It also gathers SSL/TLS certificate details and software configurations of exposed assets. As part of Cortex XSIAM, Xpanse functions as a comprehensive Attack Surface Management (ASM) platform, continuously scanning public IP addresses and domains to accurately attribute assets and enumerate internet-facing services, applications, and devices.

Prompt 4: Identification of Outdated Software – Solution should identify outdated software or insecure configurations, such as weak SSL certificates, open ports, misconfigured DNS settings, or vulnerable software versions that could be exploited by attackers.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex Xpanse identifies outdated SW and vulnerabilities related to publicly exposed assets by continuous scanning, tracking, and providing actionable insights. Xpanse enables security teams to prioritize remediation efforts & improve security posture and functions as an ASM platform, monitoring assets and enumerating internet-facing services to identify SW vulnerabilities. It patches vulnerabilities via integrations with patch management solutions or cloud providers.

Prompt 5: Integration with Vulnerability Databases – Solution should integrate with vulnerability databases such as CVE, CWE, and the National Vulnerability Database to provide immediate context around known vulnerabilities affecting identified services or software.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cortex Xpanse's Attack Surface Rules correlates discovered assets and services with vulnerabilities, automatically flagging known vulnerabilities within the Threat Response Center. This provides immediate context for prioritized remediation, enabling security teams to quickly understand the exploitability and potential impact of exposed vulnerabilities on their attack surface.

Prompt 6: Risk Scoring – Solution should accommodate risk scoring of external assets, prioritizing those that are most vulnerable to exploitation or are most critical to business operations.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

In Cortex Xpanse, you can prioritize incidents and quantify risk trends using risk scoring. Xpanse assigns a base risk score to each incident, calculated using threat and exploit intelligence relevant to the CVEs on the related service or website. If an alert is resolved or a new alert is created, Xpanse recalculates and updates the risk score. This feature is also included within Cortex XSIAM.

Prompt 7: Customizable Alerting – Solution should notify security teams when a new external asset is detected, a known vulnerability is identified, or a change in configuration occurs (e.g., a certificate has expired).

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cortex Xpanse meets this requirement with attack surface rules, which define what Xpanse looks for and the associated risk. An attack surface rule is managed by Cortex Xpanse to identify risks in an attack surface. Xpanse creates an alert whenever it detects an instance of that rule. This feature is also included within Cortex XSIAM.

Prompt 8: Integration of CTI Data Feeds – Solution should correlate external-facing assets with current threat actor campaigns or vulnerabilities that are actively being exploited. This ensures that publicly exposed services are continuously monitored against known threats in real-time.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cortex Xpanse uses data from global internet scans and open-source intelligence to maintain a complete inventory of an organization's internet-facing assets. Xpanse calculates risk scores using threat and exploit intelligence relevant to the CVEs on the related service or website (based on active classifications or web technologies) for an incident. This feature is also included in Cortex XSIAM.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SERVICE LEVEL AGREEMENT

IoT Security Service

For its IoT Security service ("Service"), Palo Alto Networks commits to using commercially reasonable efforts to achieve certain service metrics described below. In the unlikely event that Palo Alto Networks does not meet these commitments, Customers will be eligible to receive a service credit.

1. Definitions

1.1 "Available" means that the Service is capable of processing and presenting Customer's data in accordance with Service documentation.

1.2 "Available Time," in minutes, is when the Service is Available during a calendar month.

1.3 "Total Time" is the total number of minutes in a calendar month.

1.4 "Excluded Time" means the time, in minutes, described in the section entitled "Exclusions" below.

1.5 "Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during a given rolling six-month period during which the Service was not Available. The Uptime Percentage measurements exclude Exclusions. It is formulated as,

uptime percentage = available time / (total time - excluded time)

2. Service Level Commitments

Palo Alto Networks will use commercially reasonable efforts to make the Service Available with an Uptime Percentage of at least 99% during any given rolling six-month period ("Service Level"). In the event that the Service does not meet the Service Level, Customer will be eligible to request a Service credit. Service credits are calculated as a percentage of the total charges paid by Customer for the monthly billing cycle in which the Service fell below the Service Level.

Uptime Percentage	Service Credit
Less than 99% but equal to or greater than 98%	5%
Less than 98%	10%

3. Exclusions

Customer agrees and acknowledges that the IoT Security service is a tool that monitors network traffic used by certain IoT devices and is not capable of detecting intrusions or other security issues outside the normal parameters defined by Palo Alto Networks in the Service

documentation. Palo Alto Networks will attempt to monitor as much network activity as possible, but it may not be possible to monitor certain devices that are obscured behind a different intranet environment such as a layered network address table or other obstacle to intranet TCP/IP communication. Network latency and throughput may also affect the responsiveness of the Service. Palo Alto Networks is unable to monitor network traffic that is encrypted, encapsulated, tunneled, compressed or otherwise obfuscated. This Service Level Agreement shall not apply and the Service shall be deemed Available where the loss of Service results from:

(i) Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

(ii) Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;

(iii) Any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties including, but not limited to, force majeure events;

(iv) Any actions or inactions of Customer or any third party, including failure to assist in Palo Alto Networks' efforts to provide support;

(v) Planned and unplanned maintenance windows;

(vi) High Availability events and scaling events;

(vii) Fetching of logs from Cortex Data Lake service;

(viii) Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Agreement (www.paloaltonetworks.com/legal/eula).

4. Administration

4.1 Customer may, at any time, obtain Service status here (https://status.paloaltonetworks.com).

4.2 To qualify to receive Service credit under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to beta, trials and evaluations of the Service provided at no cost to the Customer.

4.3. Customer must submit a claim by opening a ticket on the Palo Alto Networks Customer Support Portal. To be eligible, the credit request must be received by Palo Alto Networks within 24 hours of an outage or an incident. Customer's failure to request and to respond to other information as required will disqualify Customer from receiving a Service credit.

4.4 When the claim is confirmed by Palo Alto Networks to be less than the Service Level, then Palo Alto Networks will issue a service credit by applying it against future Service payments due from Customer. Service credits will not entitle Customer to any refund or other payment from Palo Alto Networks.

4.5 If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the service credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer.

4.6 The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of breach of this Service Level Agreement.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term "Product" is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS "CUSTOMER", "END USER", "YOU" or "YOUR") AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS "PALO ALTO NETWORKS").

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

"Affiliate" means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where "Control" means having the power, directly

or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks' use of all Palo Alto Networks Affiliates to deliver Products and Services.

"End User Data" means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

"Enterprise Program" means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

"Hardware" means hardware-based products listed on Palo Alto Networks' then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

"Product" means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

"Published Specifications" mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. "Software" means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

"Subscription(s)" means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

"Systems Data" means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be

subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices

or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the

defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

“Confidential Information” means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party (“Discloser”), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information (“Recipient”). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and

communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include

Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the “QATT”) has been deployed in defense against, response to or recovery from an “act of terrorism” as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L4 – Service Category 4: External-Facing Asset Discovery

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Tenable Attack Surface Management

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7)
  = Total Solution Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: External-Facing Asset Discovery Solutions must help organizations identify and assess the security of their publicly accessible digital assets, such as web servers, cloud services, applications, and other internet-facing systems. The Solution must continuously scan the organization's external IP ranges and domains to identify assets that are exposed to the internet and assess their vulnerabilities.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Tenable Attack Surface Management (formerly Tenable.asm) is a comprehensive solution designed to help organizations identify & assess the security of their publicly accessible digital assets, including web servers, cloud services, applications, & other internet-facing systems. By continuously scanning external IP ranges & domains, Tenable Attack Surface Management provides visibility into assets exposed to the internet & evaluates their vulnerabilities, enabling proactive risk management. This way, organizations can comprehensively assess the security posture of their complete external attack surface.

Attack Surface Visibility: Access internet-facing assets, from web servers to IoT devices. Tenable maintains one of the largest attack surface maps, covering over 5 billion assets from 500+ sources.

Unlimited Top-Level Sources: Discover & analyze as many domains as needed to mitigate cyber risk, including potential acquisitions for due diligence.

Continuous Data Refreshes: Tenable updates terabytes of data daily or bi-weekly to reflect dynamic changes in your attack surface.

Attack Surface Change Alerts: Custom subscriptions alert you to changes in compliance, exposure, & more with over 100 event types.

Rich Asset Context: Enriches assets with over 200 metadata fields, such as CMS type & geo-IP, supporting informed decision-making.

Suggested Domains: Automatically identifies related domains, helping you discover assets you may unknowingly own.

Asset Management: Easily sort & manage assets with filters, tags, & saved views for streamlined oversight.

Documented API: A RESTful API allows for customized integrations with your security systems.

Integration with Tenable Solutions: Fully integrated with Tenable products, enabling vulnerability & web app scans for unified visibility of asset & exposure data.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Contiuous Scanning – Solution should provide continuous scanning of public IP addresses and domains associated with the organization, identifying all internet-facing services, applications, and network devices.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Tenable continuously maps the entire internet & discovers connections to your internet-facing assets so you can discover & assess the security posture of your entire external attack surface. The data & fields provided by Tenable to the customer cannot be altered or modified by the client other than by adding additional tag fields to the data. The customer can add & adjust tag fields to accommodate the type of data required.

Prompt 3: Service Detection and Banner Grabbing – Solution should collect information such as service versions, SSL/TLS certificate details, and software configurations for each exposed asset.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable will find & parse services & their corresponding versions when available using metadata, which includes (but not limited to) geolocation, operating system, open ports, service banners, TLS certificate details, etc. This technique is utilized to identify the service listening on the open port & assess any relevant Common Platform Enumeration (CPE) & Common Vulnerabilities & Exposures (CVE) information.

Prompt 4: Identification of Outdated Software – Solution should identify outdated software or insecure configurations, such as weak SSL certificates, open ports, misconfigured DNS settings, or vulnerable software versions that could be exploited by attackers.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Our solution identifies outdated software & insecure configurations. Tenable products can detect TLS/SSL certificates, assess their validity, aging, & cipher strength, & report on these aspects. Open ports are enumerated via various methods & mapped to the services running on them. Vulnerable software versions are detected & Tenable tracks the release date of each software patch to ensure software is not older than six months from the manufacturer release date.

Prompt 5: Integration with Vulnerability Databases – Solution should integrate with vulnerability databases such as CVE, CWE, and the National Vulnerability Database to provide immediate context around known vulnerabilities affecting identified services or software.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable meets this requirement by referencing the third-party databases related to each vulnerability where applicable. This can be seen in the bottom right corner of the description of each vulnerability. Third-party databases & other searchable variables include US CERT, CVE which is from the National Vulnerability Database (NVD), CVSS, Exploit DB, & OSVDB to name a few.

Prompt 6: Risk Scoring – Solution should accommodate risk scoring of external assets, prioritizing those that are most vulnerable to exploitation or are most critical to business operations.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable ranks your assets & assigns a severity level to the assets based on their security risk. The Severity column of the asset table shows the severity of an asset as Low, Medium, High, Critical, or None. Tenable Attack Surface Management calculates the severity ranking for an asset by matching the asset information with a given set of criteria. Any change or update to the asset changes the severity level of that asset.

Prompt 7: Customizable Alerting – Solution should notify security teams when a new external asset is detected, a known vulnerability is identified, or a change in configuration occurs (e.g., a certificate has expired).

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable Attack Surface Management facilitates the analysis of changes in the attack surface through subscriptions, providing automatic alerts for new & significant alterations, including real-time threat alerts for unauthorized changes or suspicious activities detected on the external attack surface.

Prompt 8: Integration of CTI Data Feeds – Solution should correlate external-facing assets with current threat actor campaigns or vulnerabilities that are actively being exploited. This ensures that publicly exposed services are continuously monitored against known threats in real-time.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Yes. Tenable offers comprehensive visibility into all of your internet-connected assets, services & applications to better understand your organization's full digital footprint & better assess & manage risk. Tenable uses its own data in t&em with third-party data sources whenever that data is relevant. Many of these data sources undergo special parsing, cleaning, transformation, & analysis to ensure that the data is conistent in both UI & API.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SLA: Uptime Guarantee: https://static.tenable.com/prod_docs/Service_Level_Agreement.pdf

Master Agreement, accepted via a click-thru acknowledgement at time of installation: https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L5 – Service Category 5: Email Security

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Abnormal Security

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Email Security Solutions must protect against email-based threats such as phishing, malware, ransomware, and email compromises. The Solution should analyze both inbound and outbound email communications in real-time, using advanced detection techniques to filter malicious content without disrupting legitimate business correspondence.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

bnormal Security provides comprehensive email protection against attacks that exploit human behavior, including malware, phishing, social engineering, ransomware, and account takeovers, with an email security platform that deeply understands human behavior.

Abnormal analyzes incoming email messages and detects potential threats in real-time. Abnormal is designed to be highly effective at identifying and blocking malicious emails, while minimizing false positives. Abnormal Security is classified as an Integrated Cloud Email Security (ICES) solution which supplements cloud email providers' (Microsoft and Google) built-in email security hygiene capabilities. Abnormal's ICES capabilities supplement these native features and utilize API access to the cloud email provider to analyze email content without the need to change the MX record.

Abnormal deeply understands human behavior to detect anomalies, protect against account takeovers, and prevent breaches. Abnormal uses a suite of neural networks and large language models to compare profiles to raw data and detect fraudulent topics, tone, and sentiment, including urgency and formality, within email content. The solution builds a relationship graph between entities both within and outside of your organization.

Abnormal, compared to other email security solutions, utilizes a modern API architecture to seamlessly integrate with M365 / GWS, using advanced AI and machine learning models to provide email security. While SEGs typically rely on rule-based filtering and known threat signatures, Abnormal employs behavioral analytics to detect subtle anomalies and identify sophisticated business email compromise attacks.

The API architecture eliminates the need for changes in MX records, ensuring it can work in parallel with email flow without disruptions. The API architecture gives Abnormal visibility on inbound email and also lateral email within an organization. Unlike SEGs which require constant updates, tuning, and rely on threat intelligence reports, Abnormal learns the different facets of emerging attacks automatically, and it autonomously adapts to how the customer interacts with email. Abnormal analyzes inbound emails against 40,000+ unique signals to detect malicious messages not only from what constitutes the attack but also from what aligns or deviates from the customer's normal email environment

Abnormal leverages multiple types of AI and machine learning models for the best security outcomes. These include a suite of neural networks, tree models, NLP, NLU, generative large language models LLMs) like GPT and discriminative LLMs like BERT. The models are used to create deep behavioral understanding for each customer, and used to detect fraudulent topics, tone, and sentiment, including urgency and formality, within email content for email protection.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Content Filtering – The Solution should break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, a nationally recognized standard, or company policy.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal utilizes a behavioral platform to judge the communication as a whole. This is the most effective method of protecting from attacks, where ones that utilize content disarm and reconstruction techniques fail. URLs contained within attachments are analyzed and Abnormal scans and extracts text from within images and other attachments. Attachments are also scanned for malware and malicious signals associated with the files are detected.

Prompt 3: Phishing Detection – Solution should analyze the email's context, structure, and metadata (e.g., header information) to detect phishing attempts, which may include spear-phishing and targeted attacks.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal provides techniques and technologies that prevent and counteract phishing attempts, unauthorized access, and theft. This includes Metadata Analysis, Uniform Resource Locator (URL) and Domain Analysis, Content Analysis, Behavioral Analysis, Real-Time Threat Intelligence. AI-Native approach to stop both credential and lateral phishing. ingests thousands of behavioral signals from multiple sources via the API architecture to detect unusual email-sending patterns.

Prompt 4: Sandboxing Technology – Solution should have the capability to safely execute email attachments and embedded links in an isolated environment to determine if they are malicious before delivery to the recipient.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Payload detection capabilities supplement behavioral analysis detection. This is the most effective method of detecting the spectrum of attacks. Sandboxing controls are bypassed by attackers through legitimate sites like SharePoint by embedding links from that site.. AI models detect and remediate malicious emails using signals including the behavior of links and attachments. There are pre-built integrations with AnyRun to provide sandboxing for threat hunting and investigation purposes.

Prompt 5: Advanced Anti Spoofing Protections – Solution should include enforcement of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to prevent sender impersonation.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal Inbound Cloud Email Security is capable of spotting all types of spoofed emails, including uncommon signs other security solutions miss. Using hundreds of thousands of signals, including DMARC and SPF, Abnormal can stop email spoofing attacks before they reach inboxes, alongside dozens of other attack types. Abnormal leverages email authentication results (SPF, DKIM, DMARC, and ARC) as inputs into the detection platform to prevent sender impersonation.

Prompt 6: Email Encryption – Solution should include encryption for sensitive communications, ensuring enforcement that messages are encrypted both in transit and at rest.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal, partnered with Microsoft/Google, delivers multiple encryption options for data in transit and data at rest. M365/GWS rules can be configured to encrypt outgoing email messages and remove encryption from messages. This includes both emails originating within your organization and replies to encrypted messages sent from your organization. Using M365/GWS + Abnormal, you can replace your traditional SEG and remain confident in how you encrypt and protect your organization's data.

Prompt 7: End-User Awareness Features – Solution should include automatic banners or warnings added to suspicious emails, helping users recognize potential threats.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal enables an organization to add banners to emails to indicate caution or draw attention to possible email risks. Customers can also choose to use the Microsoft-native and Google-native email bannering capabilities. The use of bannering and being dependent on security awareness training as primary email security controls are no longer necessary for customers that deploy Abnormal. The organization can still choose to utilize banners on the messages deemed safe by Abnormal if desired.

Prompt 8: Quarantine and Remediation Tools – Solution should provide quarantine and remediation tools for administrators, allowing them to review flagged messages, release legitimate emails mistakenly identified as threats, and block harmful content.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Abnormal customers can report False Positives through the Detection 360 page in the Portal. Abnormal has a Detection team that uses Detection 360 data to improve their AI models and provide customers with transparency into the frequency of FPs. Abnormal also locates all messages related to a misclassified case and returns FP messages to user inboxes. Flagged messages are reviewed by administrative users in the threat log, and harmful content can be blocked and removed via Search and Respond.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

ABNORMAL SECURITY CORPORATION SUPPORT AND SERVICE LEVEL AVAILABILITY POLICY

This Support and Service Level Availability Policy ("Policy") describes Abnormal Security Corporation's ("Abnormal") support offering ("Support") in connection with Customer-reported bugs, defects, or errors in the Service ("Error(s)"). Support shall be provided in accordance with the written subscription agreement under which Abnormal provides its Service as entered into by and between you ("Customer") and Abnormal ("Agreement"). Customer shall receive the level of Support set forth in this Policy or as designated in the applicable Order ("Support Level"). Abnormal may update this Policy from time to time, provided that any such update does not modify any provision of the Agreement except for this Policy. Any such updates will be posted to https://legal.abnormalsecurity.com/ or otherwise made available as set forth in the Agreement. Capitalized terms not defined in this Policy shall have the meanings given to them in the Agreement.

I. Support

1. General Support Offering. Abnormal shall provide English-speaking remote assistance to Customer Contacts (as defined below) for questions or issues arising from any Error, as further described in this Policy, including troubleshooting, diagnosis, and recommendations for potential workarounds for the duration of Customer's subscription to the applicable Service.

2. Customer Contacts. Customer shall inform Abnormal as to its approved contacts for Support, one of which must be designated as an account administrator (each, a "Customer Contact"). Customer is solely responsible for maintaining an accurate list of Customer Contacts with Abnormal, including names and contact information. Abnormal assumes no responsibility for Support Cases that cannot be addressed due to a lack of updated Customer Contact information.

3. Submitting Support Cases. Customer Contacts must use reasonable diligence to ensure a perceived Error is not an issue with Customer's own equipment, software, or internet connectivity prior to requesting Support. Customer Contacts may contact Support by submitting a Support request (each, a "Support Case") to: (a) the support portal located at https://support.abnormalsecurity.com (or such successor URL as may be designated by Abnormal) (such website, the "Support Portal") or (b) the web interface as described in the Documentation. If Customer Contacts cannot access the Support Portal they may open a Support Case by emailing support@abnormalsecurity.com or, in the event Customer Contacts cannot access the Support Portal or email, they may contact Abnormal Support by phone solely for purposes of having the Support Case submitted on their behalf. All Customer Contacts must be familiar with the Documentation and be reasonably trained in the use and functionality of the

Service. Customer Contacts will assist Abnormal to resolve Support Cases by complying with the Customer obligations set forth in Table 1.

4. Support Cases. Each Support Case shall: (a) designate the Severity Level of the Error in accordance with the definitions in Table 1; (b) identify the Customer account that experienced the error; (c) include information sufficiently detailed to allow Abnormal to attempt to duplicate the Error (including any relevant error messages, but not export-controlled data, personal data (other than as required herein), sensitive data, other regulated data, or Customer Data); and (d) identify the Customer Contact most familiar with the issue. The Customer Contact shall also give Abnormal any other important Support Case information requested by Abnormal in a timely manner. Unless Customer expressly designates the Severity Level, the Support Case will default to Severity Level 4. If Customer Contacts submit Support Cases related to enhancement or feature requests, Abnormal shall treat those tickets as closed once the request has been forwarded internally.

Table 1: Error Severity Level Definitions and Initial Response Times

Error Severity Level

Description Initial Response Time Target Customer Responsibility

Severity Level 1

(Urgent)

An Error that causes a (a) service disruption or (b) degraded condition that renders the Service inoperable. One (1) Hour Commit appropriate resources to provide additional information as needed. Make reasonable efforts to apply solutions quickly.

Severity Level 2

(High)

An Error that (a) causes the Service to operate in a degraded condition with a high impact to key portions of the Service or (b) seriously impairs Customer’s use of material function(s) of the Service and Customer cannot reasonably circumvent or avoid the Error without the expenditure of significant time or effort. Two (2) Business Hours Commit appropriate resources to be available to provide additional information as needed. Make reasonable efforts to apply solutions upon receipt.

Severity Level 3

(Normal)	An Error that has a medium-to-low impact on the Service. The Service is (a) running with limited functionality in one or more areas or (b) experiencing intermittent issues. Customer can access and use the material functionality of the Service.	Eight (8) Business Hours	Monitor and respond as necessary.
Severity Level 4 (Low)	How-to questions and Service issues with no Service degradation.	One (1) Business Day	Monitor and respond as necessary.
RFE	Requests for enhancements to the Service.	Two (2) Business Days	N/A

5. Other Support and Training. Abnormal also offers various support and training resources such as documentation, FAQs and user guides available on the Abnormal Community.

6. Error Response. Abnormal Support will investigate Errors and assign the applicable Severity Level listed in Table 1. If Abnormal's Severity Level designation is different from that assigned by Customer, Abnormal will promptly notify Customer of such designation. If Customer notifies Abnormal of a reasonable basis for disagreeing with Abnormal's designated Severity Level, the parties each will make a good faith effort to discuss, escalate internally, and mutually agree on the appropriate Severity Level. Abnormal shall use commercially reasonable efforts to meet the Initial Response Time Target for the applicable Severity Level, as measured during the Support hours set forth in Table 2 below (with the total Business Hours in an in-region support day each a "Business Day").

Table 2: Support Hours

Region	Americas	EMEA	Asia Pacific
Severity 1	24 x 7 x 365	24 x 7 x 365	24 x 7 x 365
Severity 2-4	6AM-6PM PT Mon-Fri	8AM-5PM GMT Mon-Fri	8AM-5PM AEDT Mon-Fri
Exclusions	U.S. Federal Holidays	United Kingdom Public and Bank Holidays	Australian National and Public Holidays

II. Service Level Agreement

The Monthly Availability Percentage for the Service is ninety-nine and nine-tenths percent (99.9%) ("Service Level"). If the Service does not meet the Service Level in a given month ("Service Level Failure"), then as Customer's sole and exclusive remedy, Customer shall be eligible to receive the applicable number of Service level credits set forth in Table 3 below ("Service Level Credits"), credited towards extending Customer's Subscription Term at no charge, provided that Customer requests Service Level Credits within thirty (30) days from the time Customer becomes eligible to receive Service Level Credits under this Policy by filing a Support Case. Failure to comply with this notification requirement will forfeit Customer's right to receive Service Level Credits. The aggregate maximum amount of Service Level Credits for a Service Level Failure will not exceed 15 days per month. Service Level Credits may not be exchanged for, or converted to, monetary amounts. Customer may request the Service Level attainment for the previous month by filing a Support Case.

Table 3: Service Level Credits

Monthly Availability Percentage	Service Level Credit
< 99.9% - ≥ 98.0%	3 Days
< 98.0% - ≥ 95.0%	7 Days
< 95.0%	15 Days

Policy Exclusions

Abnormal will have no liability for any failure to meet the Service Level to the extent arising from: (a) Planned Maintenance or Emergency Maintenance; (b) third-party platforms and networks, Customer or User application, equipment, software or other third-party technology; (c) Customer or its User's use of the Service in violation of the Agreement or not in accordance with the Documentation; (d) force majeure events — i.e., any cause beyond such party's reasonable control, including but not limited to acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, public health emergencies (including pandemics and epidemics), acts or orders of government, acts of terrorism, or war; or (e) any access to the Service (or Service features) on a free, trial, beta or early access basis, or due to suspension, limitation, and/or termination of Customer's access or use of the Service in accordance with its Agreement.

Definitions:

"Calendar Minutes" is defined as the total number of minutes in a given calendar month.

"Emergency Maintenance" means circumstances where maintenance is necessary to prevent imminent harm to the Service, including critical security patching.

"Monthly Availability Percentage" is defined as the difference between Calendar Minutes and the Unavailable Minutes, divided by Calendar Minutes, and multiplied by one hundred (100).

"Planned Maintenance" means routine maintenance periods that continue for no more than four hours in any one instance, so long as Abnormal provides at least 48 hours prior notice (including by email) to Customer.

"Unavailable" means if Customer is unable to access the Service by means of a web browser and/or API as a result of failure(s) in the Service, as confirmed by Abnormal.

"Unavailable Minutes" is defined as the total accumulated minutes when the Service is Unavailable.

ABNORMAL SECURITY CORPORATION INFORMATION SECURITY POLICY

This Information Security Policy ("Policy") is incorporated into the subscription agreement under which Abnormal Security Corporation ("Abnormal", "we", or "us") provides its Service ("Agreement") to the Party listed as Customer on the Agreement ("Customer") and describes Abnormal's Information Security Program ("Security Program") which Abnormal has implemented and will maintain in accordance with this Policy.

Abnormal may update this Policy from time to time, provided that any such update does not: (i) modify any provision of the Agreement except for this Policy; or (ii) materially diminish the overall security protections described herein during the Subscription Term. Any such updates will be posted to https://legal.abnormalsecurity.com/. Capitalized terms not otherwise defined in this Policy shall have the meanings given to them in the Agreement. Any ambiguity, conflict or inconsistency between this Policy, the Agreement, the DPA, or other document comprising this Agreement shall be resolved according to the following order of precedence: (1) DPA; (2) this Policy; (3) the Agreement; and (4) other supplementary documents incorporated into the Agreement.

Minimum Security Standards. The Security Program will use industry-standard controls designed to protect the confidentiality, integrity, and availability of Customer Data against anticipated or actual threats or hazards; accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or damage. The Security Program will use administrative, technical, and physical safeguards appropriate to: (a) the size, scope, and type of Abnormal's business; (b) the type of information that Abnormal processes on behalf of Customer (where such information is provided to Abnormal in accordance with the Agreement); and (c) the corresponding need for security and confidentiality of such information.

For more details on Abnormal's Security Program, please see the Security Hub at security.abnormalsecurity.com ("Security Hub").

Service Infrastructure. The Service and Customer Data are hosted on infrastructure using industry-leading cloud hosting providers. No Customer Data is stored or processed in Abnormal office facilities.

Elements of the Security Program.

1. Policies and Procedures. Abnormal has implemented and will maintain security, privacy, confidentiality, availability, and code of conduct policies and procedures designed to ensure that the Service and Abnormal's employees and contractors ("Personnel") process Customer Data in accordance with this Policy and the Agreement. Abnormal has implemented and will enforce

disciplinary measures against Personnel for failure to abide by the aforementioned policies and procedures.

2. Logical Access Controls. Abnormal will take reasonable measures that are designed to ensure appropriate user authentication for Personnel with access to Customer Data, including without limitation, by assigning each Personnel unique authentication credentials for accessing any system on which Customer Data is processed and prohibiting Personnel from sharing their authentication credentials. Abnormal will restrict access to Customer Data solely to those Personnel who need access to Customer Data to perform Abnormal's obligations under the Agreement.

Further, Abnormal will take reasonable measures to implement and maintain logging and monitoring technologies designed to help detect and prevent unauthorized access to its networks, servers, and applications, including but not limited to those that process Customer Data. Abnormal will conduct periodic reviews of systems that process Customer Data to verify the identities of individuals who access and have privileged access to systems to help detect and prevent unauthorized access to its network, servers, and applications and verify that all changes to its authentication systems were authorized and correct. Abnormal has implemented and will maintain procedures and policies that are designed to ensure that, upon termination of any Personnel the terminated user access to any Customer Data on Abnormal systems will be promptly revoked, and in all cases, revocation will occur no later than twenty-four (24) hours following such termination.

3. Intrusion Prevention. Abnormal utilizes reasonable measures designed to ensure that its infrastructure protections are consistent with industry standards in preventing unauthorized access to Abnormal networks, servers, and applications. Such measures include but are not limited to the implementation of intrusion prevention technologies, anti-malware services, and firewall rules.

4. Physical Access. Abnormal limits physical access to its office facilities using physical controls (e.g., coded badge access). Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that access to their data centers and other areas where Customer Data is stored is limited to authorized individuals. Cloud hosting provider data centers and Abnormal office facilities leverage camera or video surveillance systems at critical internal and external entry points and are monitored by security Personnel.

5. Environmental Protection. Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that cloud hosting provider data centers implement and maintain appropriate and reasonable environmental controls for its data centers and other areas where Customer Data is stored, such as air temperature and humidity controls, and protections against power failures.

6. Backup, Disaster Recovery, and Business Continuity. Abnormal will: (a) back up its production file systems and databases according to a defined schedule and conduct regular testing of backups; and (b) maintain a disaster recovery plan for the production data center and maintain business continuity plans designed to manage and minimize the effects of disaster events or unplanned operational disruptions with a stated goal of resuming routine service within forty-eight (48) hours; and (c) conduct regular testing of the effectiveness of such plans.

7. Security Incident Response. For purposes of this Policy, any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data is a "Security Incident". Abnormal will: (a) take reasonable measures to implement and maintain logging and monitoring technologies designed to identify, alert, and analyze security events; and (b) maintain plans and procedures to be followed in the event of an actual or suspected Security Incident ("Incident Response Plans"). The Incident Response Plans require Abnormal to undertake a root cause analysis of any actual or suspected Security Incident and to document remediation measures.

8. Security Incident Notification. Abnormal will implement and follow procedures that are designed to detect and respond to Security Incidents and will notify Customer of any Security Incident affecting its Customer Data within forty-eight (48) hours of Abnormal becoming aware of the Security Incident, regardless of whether the Security Incident triggers any applicable breach notification law. Such notification will be executed using the contact information provided by Customer under the Records and Validation section of the Agreement.

Notice to a Customer will include: (a) a description of the nature of the Security Incident, including the categories and approximate number of Customer's data subjects and personal data records concerned; (b) the name of Abnormal's contact where more information can be obtained; (c) a description of the likely consequences of the Security Incident; (d) a description of the measures taken or proposed to address or mitigate the adverse effects of the Security Incident, to the extent within Abnormal's reasonable control.

9. Storage and Transmission Security. Abnormal will logically segregate Customer Data from all other Abnormal or third-party data. Abnormal will: (a) securely store Customer Data; (b) encrypt Customer Data during transmission using, at a minimum, Transport Layer Security (TLS) protocol version 1.2 or above; and (c) encrypt Customer Data at rest using, at a minimum, the Advanced Encryption Standard (AES) 256-bit encryption protocol. Abnormal will establish encryption key management processes that are designed to ensure the secure generation, storage, distribution, and destruction of encryption keys. Abnormal will not store Customer Data on any removable storage devices or other similar portable electronic media.

10. Data Retention and Secure Disposal. Abnormal will retain and securely dispose of Customer Data in accordance with the Agreement. During the Subscription Term, Customer may through the features of the Service access, return to itself or delete Customer Data. Following termination or expiration of the Agreement, Abnormal will delete all Customer Data from Abnormal's systems. Deletion will be in accordance with industry-standard secure deletion practices. Abnormal will issue a certificate of deletion upon Customer's written request. Notwithstanding the foregoing, Abnormal may retain Customer Data: (a) as required by applicable laws, or (b) in accordance with its standard backup or record retention policies, as governed by the Agreement.

11. Risk Identification and Assessment. Abnormal will implement and maintain a risk assessment program to help identify foreseeable internal and external risks to Abnormal's information resources and to Customer Data, and determine if existing controls, policies, and procedures are adequate.

12. Subprocessors. Abnormal will authorize third-party service providers to access or process Customer Data ("Subprocessors") only in accordance with the requirements and procedures specified in the Agreement, and specifically in the DPA. Prior to authorizing Subprocessors, Abnormal security Personnel will conduct a risk assessment of each Subprocessor to seek assurances of its data security practices (e.g., in the form of an independent third-party audit report such as the SOC 2 Type 2, ISO 27001, or a vendor security and risk evaluation). Abnormal enters into written agreements with its Subprocessors with security and data processing obligations substantially the same as those contained in this Policy.

13. Change and Configuration Management. Abnormal has implemented and will maintain processes for managing changes and updates to production systems, applications, and databases, including without limitation, processes for documenting, testing, and approval of changes into production, security patching, and authentication.

14. Release Management. Abnormal follows a continuous release process versus a standard release schedule and does not require a maintenance downtime window for the Service when pushing a new release. No Customer interaction is required to upgrade to the new version; the release is automatically applied to all Customers. Releases follow Abnormal's change management procedures that are designed to ensure that releases are tested and approved prior to push to production. Abnormal communicates release information using the notification functionality within the Service.

15. Training. Abnormal will undertake the following measures that are designed to ensure that Personnel who will have access to Customer Data are appropriately qualified and trained to handle Customer Data:

15.1. Information Security and Privacy Awareness Training. Upon hire and at minimum annually thereafter, Abnormal will require security and privacy awareness training to all Personnel who will process or have access to Customer Data. Abnormal security and privacy awareness training is designed to meet industry standards and will include, at a minimum, education on safeguarding against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and social engineering mechanisms.

15.2. Secure Code Training. Abnormal will require annual training on secure coding principles and their application at minimum annually to all Personnel who develop or handle any Abnormal source code. Abnormal secure code training will cover topics such as: (a) the Open Web Application Security Project list of the 10 most critical security risks to web-based applications (OWASP Top 10); and (b) appropriate techniques for the remediation of the listed security vulnerabilities.

16. Background Checks. Abnormal Personnel will undergo a civil and criminal background check, to the extent permitted by applicable law.

17. Audit and Assessments. Abnormal has implemented and will maintain a Compliance Audit Program including assessments performed by an independent third-party (“Auditor”) and defined Customer audit rights in accordance with the Agreement.

17.1 Independent Security Audit. Abnormal will engage an Auditor to certify compliance with the ISO 27001 standard, and conduct a SOC 2 Type 2 audit with a scoped audit period of a maximum 12 months to demonstrate its compliance with the security requirements of the Security Program. Abnormal’s SOC 2 Type 2 audit covers the Trust Services Criteria of Security, Availability, Confidentiality, and Privacy. Abnormal will make available to Customer publicly available certificates and summary copies of its SOC 2 Type 2 audit report (each, an “Audit Report”) on the Security Hub.

17.2 Customer Audits. Abnormal will make available the information necessary to demonstrate its compliance with the Security Program to support Customer in obtaining the information necessary to complete Customer’s audits, reviews, risk assessments, and security-related questions of Abnormal as Customer’s vendor. Please see the Security Hub for this information. For further details on Customer audit rights, please see your Data Processing Addendum (DPA).

17.3 Penetration Tests. At least once per twelve (12) month period, Abnormal will undertake a network penetration test by an independent third-party. Abnormal will make available to Customer an executive summary section of the penetration test report that pertains to the systems and operations that process, store, or transmit Customer Data. Abnormal will remediate all vulnerabilities that the penetration test identifies in accordance with the following remediation timelines:

Level	Timeline
Critical	15 days
High	30 days
Medium	60 days
Low	Reasonable timeframe based on nature and probability of exploitation

All information exchanged between the Parties in the course of the activities described in all Sections above are deemed to be Abnormal Confidential Information.

Abnormal Security Acceptable Use Policy

This Acceptable Use Policy (“AUP”) describes the prohibited uses of the Software as a Service offering (the "Service") provided by Abnormal Security Corporation (“Abnormal"). This AUP is in addition to any other terms and conditions under which Abnormal provides the Service to you. In addition to any other remedies available to Abnormal, if Abnormal determines in its sole discretion that you violate the AUP, we may suspend, limit, or terminate your use of the Service without prior notice or liability. This right applies, even if the breach is unintentional or unauthorized, if we believe that any such suspension, limitation, or termination is necessary to ensure compliance with laws, or to protect the rights, safety, privacy, security, or property (including the Service) of Abnormal or others.

Abnormal may modify this AUP at any time by posting an updated version of this document. Such updates will be effective upon posting. We therefore recommend that you visit the Abnormal website regularly to ensure that your activities conform to the most recent version. Your continued access to and use of the Service constitutes your agreement to be bound by such updates.

The prohibited uses listed below are not exhaustive. Prohibited uses and activities by you, the customer, your users or any third party include, without limitation:

- Violating any applicable laws or regulations (including without limitation data, privacy, and export control laws) or use the Service in a manner that gives rise to civil or criminal liability;

- Intentionally distributing malicious code, viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive manner;

- Infringing or misappropriating Abnormal’s or any third party’s intellectual property, proprietary or privacy rights;

- Reverse engineering, decompiling, or disassembling the Service or any software used in the provision of the Service;

- Interrupting, or attempting to interrupt, violate, obtain unauthorized access to, disrupt, damage, overburden, breach, or compromise the operation or security of the Service or any networks or systems;

- Using the Service for any reason other than as intended by the parties.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L5 – Service Category 5: Email Security

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Proofpoint Adaptive Email Security

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Email Security Solutions must protect against email-based threats such as phishing, malware, ransomware, and email compromises. The Solution should analyze both inbound and outbound email communications in real-time, using advanced detection techniques to filter malicious content without disrupting legitimate business correspondence.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Proofpoint's Adaptive Email Solutions use AI to defend against advanced phishing threats and protect sensitive data on email.

For inbound email protection, Adaptive Email Security uses AI based behavioral and content analysis, alongside the largest global email threat dataset to stop advanced phishing attacks. It checks hundreds of data points on every email using relationship graphs, deep learning, LLMs, NLP and more, with integrated threat intelligence from more than 2.8T emails annually. It leverages threat data from trillions of emails to identify malicious URLs and attachments. It can also detect spikes in email volume and anomalous communications when compared with historical email patterns.

Adaptive Email Security uses AI to make predictions based on email metadata, content in the email body, and historical email patterns. Its AI ensemble produces a confidence score, indicating confidence in the detection of a true positive threat. Organizations can use this confidence score to determine the best form of remediation, among several options, to filter out malicious content without disrupting legitimate business correspondence.

Within AES, high confidence score emails can be "admin quarantined" or automatically removed from users' inboxes. Lower confidence emails can be "user quarantined", in which they're held in a hidden folder in the employee's email account. AES sends a "defanged" copy of the email to the employee's inbox with an alert notification, alerting them that the flagged email is potentially malicious and the top three threat signals observed in the AES analysis. The user can then decide to delete the email or release it to their inbox.

For outbound email protection, Adaptive Email DLP uses behavioral AI to automatically prevent accidental and intentional data loss over email. It warns users of an incorrect recipient or attachment before an email is sent. It leverages end user behavior to analyze email recipients, subject lines, content, attachments and detects anomalies such as whether the email salutation is commonly used, if the topics and content of the email are relevant to the recipient, and if there are any other recipients usually seen on emails together. With intuitive warnings that provide context for why potentially mis-addressed emails are blocked, it empowers end users to make informed decisions.

Adaptive Email DLP also detects and stops sensitive or restricted data from being sent to unauthorized or freemail accounts without disrupting user productivity and with near-zero administration overhead. It automatically detect legal, financial, HR terms, and sensitive documents, and create intelligent policies that blend machine learning with custom rules to prevent sensitive data loss. With intuitive warnings that provide context for why potentially harmful emails are blocked, it protects enterprises while empowering end users to make informed decisions about what they are sending.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Content Filtering – The Solution should break down files to their discrete components in real-time and reconstruct a clean version of the email, removing anything that doesn't conform with the file type specifications, a nationally recognized standard, or company policy.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Adaptive Email DLP uses machine learning to detect sensitive content being sent to unauthorized email addresses. It scans inside of emails and attachments for project references and identifiers, and uses a sensitivity algorithm to scan attachments for sensitive keywords. It scans all Microsoft Office files, PDF, RTD, archive files, txt, csv, UTF-7/8/16/32 and more. On detection, it warns or block users from sending emails that don't conform to specifications, standards or policies.

Prompt 3: Phishing Detection – Solution should analyze the email's context, structure, and metadata (e.g., header information) to detect phishing attempts, which may include spear-phishing and targeted attacks.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

To detect phishing, Adaptive Email Security uses methods like topic clustering, natural language processing, large language models and OCR to break down email body and attachment content. It identifies unusual text in images, QR codes, URLs, subject headings, body text, and malicious content inside of email attachments for potential threats. It uses LLMs for advanced intent analysis, labeling emails by topics such as credentials, services, financial, BEC, phishing, proposals and more.

Prompt 4: Sandboxing Technology – Solution should have the capability to safely execute email attachments and embedded links in an isolated environment to determine if they are malicious before delivery to the recipient.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

In Q1 of 2025, Adaptive Email Security will sandbox attachments and embedded links. This development provides exhaustive analysis via static, dynamic and analyst-assisted execution. It first use ML-driven intelligence to determine whether payloads should be sent to the sandbox for further analysis. Emails containing suspicious attachments and URLs will be removed, post-delivery from the users inbox. Emails containing suspicious URLs may also be rewritten, by configuration.

Prompt 5: Advanced Anti Spoofing Protections – Solution should include enforcement of Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols to prevent sender impersonation.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Adaptive Email Security doesn't enforce email authentication protocols as it is not a secure email gateway. Sender authentication checks are leveraged in tuning the confidence score of a particular email, but emails aren't flagged solely due to their authentication status.

Prompt 6: Email Encryption – Solution should include encryption for sensitive communications, ensuring enforcement that messages are encrypted both in transit and at rest.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Proofpoint's Adaptive Email solutions don't provide outbound encryption capabilities for sensitive communications today.

Prompt 7: End-User Awareness Features – Solution should include automatic banners or warnings added to suspicious emails, helping users recognize potential threats.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

In AES, low-medium confidence detections can be "user quarantined", in which they're held in a hidden folder in the employee's email account. AES sends a "defanged" copy of the email to the employee's inbox with an automatic warning banner, alerting them that the email is potentially malicious, including the top threat signals observed. The "defanging" of the email effectively neutralizes hyperlinks and removes attachments until the user decide to delete the email or release it to their inbox.

Prompt 8: Quarantine and Remediation Tools – Solution should provide quarantine and remediation tools for administrators, allowing them to review flagged messages, release legitimate emails mistakenly identified as threats, and block harmful content.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Quarantine and remediation is configurable by confidence level. Threats can by automatically removed for admin review or replaced with a defanged copy/contextual warning banner depending on configuration. Admins can review and release emails individually or in bulk, which trains the ML models on mistakes to avoid in the future. Emails reported by end users are automatically classified and triaged by adaptive email security. If classified as safe, reported emails are automatically remediated.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

STATE AND LOCAL / HIGHER ED (SLED) END USER LICENSE TERMS

These SLED End User License Terms shall apply to the use of Proofpoint Products by Customer pursuant to a subscription license.

1. Definitions. The following terms apply to each Public Sector Customer (“Customer”) license of Proofpoint Products from the Public Sector Reseller or Distributor (“Contractor”) under the applicable government prime contract:

“Customer” means only the public sector agency which has purchased the Proofpoint Product subscription license for its internal purposes and does not include any other agency or governmental subdivision unless expressly stated in this Agreement or the Proofpoint quote accompanying the purchase order.

“Documentation” means the technical description of the Proofpoint Product(s) contained in the then- current Product Terms.

"Proofpoint Products" means the appliance, service or software listed in the Contractor’s Schedule Price List by and licensed by Customer from Proofpoint, Inc. (“Proofpoint”) pursuant to a Customer Purchase Order (“Order”).

“Product Terms” means the descriptions of Proofpoint Products and related terms contained at https://www.proofpoint.com/us/legal/license/product-terms that are hereby incorporated herein by reference and made a part hereof.

"Service" means any Proofpoint Product licensed on a hosted basis as software-as-a-service.

"Software" means any Proofpoint binary software programs licensed by Proofpoint to Customer, together with all the Software Updates.

“User” means Customer's employees, agents, contractors, consultants or other individuals who are licensed to use the Proofpoint Product, and each User must be assigned a separate account on Customer’s email server for sending or receiving messages or data within Customer’s email system or network, or if applicable, login credentials for Customer’s social media accounts.

2, License.

Customer is granted a limited term, non-sublicensable, non-transferable, and non- exclusive license to access or use the Proofpoint Products licensed by Customer from Contractor during the applicable subscription term, for its intended purposes, solely for Customer's internal business purposes and not for further use by or disclosure to third parties and in accordance with the Proofpoint Products Documentation and any applicable laws or regulations. Customer's right to access or use Proofpoint Products is limited to those parameters set forth in the applicable Order provided to Proofpoint including, but not limited to the maximum number of Users ("Licensed User Count") (and storage if applicable) for each module and the type of deployment (i.e., SaaS or appliance).

3. License Restrictions.

Customer will not and will not allow any third party to:

a) copy, modify, or create derivative works of the Proofpoint Products or Proofpoint Products Documentation;

b) reverse engineer, decompile, translate, disassemble, or discover the source code of all or any portion of the Proofpoint Products except and only to the extent permitted by applicable federal law notwithstanding this limitation, provided however, that in any case, Customer shall notify Proofpoint in writing prior to any such action and give Proofpoint reasonable time to adequately understand and meet the requested need without such action being taken by Customer;

c) remove, alter, cover or obscure any notice or mark that appears on the Proofpoint Products or on any copies or media;

d) sublicense, distribute, disclose, rent, lease or transfer to any third party any Proofpoint Products;

e) export any Proofpoint Products in violation of U.S. laws and regulations;

f) attempt to gain unauthorized access to, or disrupt the integrity or performance of, a Proofpoint Product or the data contained therein;

g) access a Proofpoint Product for the purpose of building a competitive product or service or copying its features or user interface;

h) use a Proofpoint Product, or permit it to be used, for purposes of: (a) product evaluation, benchmarking or other comparative analysis intended for publication outside the Customer's organization without Proofpoint's prior written consent; (b) infringement or misappropriation of the intellectual property rights of any third party or any rights of publicity (e.g. a person's image, identity, and likeness) or privacy; (c) violation of any federal law, statute, ordinance, or regulation (including, but not limited to, the laws and regulations governing export/import control, unfair competition, anti- discrimination, and/or false advertising); (d) propagation of any virus, worms, Trojan horses, or other programming routine intended to damage any system or data; and/or (e) filing copyright or patent applications that include the Proofpoint Product and/or Documentation or any portion thereof; or

i) upload or download, post, publish, retrieve, transmit, or otherwise reproduce, distribute or provide access to information, software or other material which: (i) is confidential or is protected by copyright or other intellectual property rights, without prior authorization from the rights holder(s);

(ii) is defamatory, obscene, contains child pornography or hate literature; or (iii) constitutes invasion of privacy, appropriation of personality (e.g. image, identity, likeness), or unauthorized linking or framing.

Proofpoint Products are for use with normal business messaging traffic only, and Customer shall not use the Proofpoint Products for the machine generated message delivery of bulk, unsolicited emails or in any other manner not prescribed by the applicable Proofpoint Products Documentation. Proofpoint shall have the right to monitor and reset harmful outbound email configuration settings impacting the Proofpoint platform.

4. Customer Responsibilities.

Customer is responsible for (i) all activities conducted under its user logins; (ii) obtaining and maintaining any Customer equipment and any ancillary services needed to connect to, access or otherwise use the Proofpoint Products and ensuring that the Customer equipment and any ancillary services are (a) compatible with the Proofpoint Products and (b) comply with all configuration requirements set forth in the applicable Proofpoint Product Documentation; and (iii) complying with all federal laws, rules and regulations regarding the management and administration of its electronic messaging system, including but not limited to, obtaining any required consents and/or acknowledgements from its employees, agents, consultants and/or independent contractors (collectively referred to as "personnel," hereinafter) and service providers (if applicable) in managing its electronic messaging system and/or social media systems (as applicable). Customer shall be solely responsible for any damage or loss to a third party resulting from the Customer's data, or where Customer's use of the Proofpoint Products are in violation of federal law, or of this Agreement, or infringe the intellectual property rights of, or has otherwise harmed, such third party.

Customer shall (i) take all necessary measures to ensure that its users use Proofpoint Products in accordance with the terms and conditions of this Agreement; and (ii) in the case of any purchase of Proofpoint Secure Share, users of the Proofpoint Product will need to register to use the Secure Share. For the purposes of Proofpoint's compliance with its obligations under this Agreement, Customer consents to and authorizes Proofpoint (and its authorized subcontractors, subject to approval by the Contracting Officer) to retain, store and transmit any Customer information and data, subject to

Government security requirements that Customer discloses to Proofpoint and pursuant to the normal functioning of Proofpoint Products. Customer information and data includes, but is not limited to (i) all configuration, rules and policies executed at Customer's direction; (ii) any document management or retention protocols that would delete, track, transmit or route documents or other data; (iii) any requests by Customer or required hereunder for log, access, support-related or other transmissions under this Agreement.

5. Data Security & Privacy

5.1 Limited Use of Personal Data. Proofpoint and its subsidiaries are authorized to access and process Personal Data solely in accordance with the terms of the Agreement. Proofpoint and its subsidiaries shall take reasonable steps to ensure the reliability of any employee, agent or subcontractor who may have access to the Personal Data and will ensure access is strictly limited to those individuals who need to access the relevant Personal Data in the performance of Proofpoint's obligations under the Agreement.

5.2 Data Safeguards. Proofpoint will maintain reasonable administrative, physical, and technical safeguards for protection of the security and confidentiality of Customer Data and Personal Data, including, but not be limited to, measures for preventing unauthorized access, use, modification or disclosure of Customer Data and Personal Data. Proofpoint will comply with its Data Security, Protection, Audit and Compliance Policy at https://www.proofpoint.com/us/legal/license when processing any Customer Data and Personal Data.

5.3 "Customer Data" means the Customer specific configurations and rules implemented in the Proofpoint Products, and any Customer content processed by the Proofpoint Products (e.g., email text and attachments) that is not Personal Data. "Personal Data" means data about an identifiable individual that is protected by privacy laws where the individual resides. Examples of personal data include name, religion, gender, financial information, national identifier numbers, health information, email addresses, IP addresses, online identifiers and location data.

6. Confidentiality

6.1 Receiving Party shall not (i) disclose any Confidential Information of the Disclosing Party to any third party, except as otherwise expressly permitted herein, or (ii) use any Confidential Information of Disclosing Party for any purpose outside the scope of the Agreement, except with Disclosing Party's prior written consent. The Receiving Party shall not make Confidential Information available to any of its employees or consultants except those that have agreed to obligations of confidentiality at least as restrictive as those set forth herein and have a "need to know" such Confidential Information. The Receiving Party agrees to hold the Disclosing Party's Confidential Information in confidence and to take all precautions to protect such Confidential Information that the Receiving Party employs with respect to its own Confidential Information of a like nature, but in no case shall the Receiving Party employ less than reasonable precautions. The Agreement will not be construed to prohibit disclosure of Confidential Information to the extent that such disclosure is required to by law or valid order of a court or other governmental authority; provided, however, to the extent permitted by law, the responding party shall give prompt written notice to the other party to enable the other party to seek a protective order or otherwise prevent or restrict such disclosure and, if disclosed, the scope of such disclosure is limited to the extent possible.

6.2 The Receiving Party will return all copies of the Disclosing Party's Confidential Information upon the earlier of (i) the Disclosing Party's request, or (ii) the termination or expiration of the Agreement. Instead of returning such Confidential Information, the Receiving Party may destroy all copies of such Confidential Information in its possession; provided, however, the Receiving Party may retain a copy of any Confidential Information disclosed to it solely for archival purposes, provided that such copy is retained in secure storage and held in the strictest confidence for so long as the Confidential Information remains in the possession of the Receiving Party.

6.3 The parties acknowledge and agree that the confidentiality obligations set forth in this Master Agreement are reasonable and necessary for the protection of the parties' business interests, that irreparable injury may result if such obligations are breached, and that, in the event of any actual or potential breach of this Confidentiality provision, the non-breaching party may have no adequate remedy at law and shall be entitled to seek injunctive and/or other equitable relief as may be deemed proper by a court of competent jurisdiction.

6.4 "Confidential Information" means all confidential and proprietary information of a party ("Disclosing Party") disclosed to the other party ("Receiving Party"), whether orally or in writing, that is designated as "confidential" or the like, or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including the terms and conditions of the Agreement (including pricing and other terms reflected in a Purchase Order), the Proofpoint Products business and marketing plans, technology and technical information, product designs, and business processes. "Confidential Information" shall not include information that (i) is or becomes a matter of public knowledge through no act or omission of the Receiving Party; (ii) was in the Receiving Party's lawful possession prior to the disclosure without restriction on disclosure; (iii) is lawfully disclosed to the Receiving Party by a third party that lawfully and rightfully possesses such information without restriction on disclosure; (iv) the Receiving Party can document resulted from its own research and development, independent of receipt of the disclosure from the Disclosing Party; or (v) is disclosed with the prior written approval of the Disclosing Party.

7. Support and Service Levels.

7.1 Support Services. Proofpoint shall provide support and/or Managed Services provided Customer is current in payment of the applicable Subscription Fees and any additional fees for support and/or Managed Services, if applicable. Proofpoint's current support terms are described on Proofpoint's website at https://www.proofpoint.com/us/legal/license.

7.2 Service Levels. Proofpoint provides a Service Level Agreement ("SLA") for the applicable Proofpoint Service. The SLA is posted on Proofpoint's website at http://www.proofpoint.com/license. In the event of a breach of an SLA, as Customer's sole and exclusive remedy, Proofpoint shall provide the remedy set forth in the applicable SLA.

8. Reporting and Audit.

Customer shall monitor and report its actual usage of the subscription-based Proofpoint Products (“License Count”). A “Base License” is the number of Licenses for which Customer has paid Subscription Fees. Customer will provide Proofpoint with a License Count on or before the date on which the then- current License Count exceeds the Base License Count by ten percent (10%) or more (if applicable) by email at accountsreceivable@proofpoint.com. Proofpoint may also at any time produce an actual license count for verification by Customer. If, in either case, the License Count is greater than the Base License, Customer shall pay the Contractor upon receipt of an invoice for each License beyond the Base License from the time such Licenses were activated through the remainder of the Initial Term or Extension Term, as applicable.

9. Warranty.

9.1 Warranties and Remedies.

(a) Performance Warranties. Proofpoint warrants that during the Subscription Term the applicable Service (“SaaS Warranty”) and Software (“Software Warranty”) will substantially conform in all material respects to the Documentation. Customer will provide prompt written notice of any non-conformity. Proofpoint may modify the Documentation in its sole discretion. The Software Warranty does not apply to:

(a) Software that has been modified by any party other than Proofpoint; or (b) Software that has been improperly installed or used in a manner other than as authorized under the Agreement.

(b) SaaS and Software Warranty Remedy. As Customer’s sole and exclusive remedy and Proofpoint’s entire liability for any breach of the SaaS Warranty or the Software Warranty, Proofpoint will

(a) use reasonable efforts to fix, provide a work around, or otherwise repair or replace the Service or Software, as applicable, or if Proofpoint is unable to do so, (b) terminate the license to use such component of the Service or the applicable Software and return the Subscription Fees paid to Proofpoint for such allegedly defective Service or Software, as applicable, for the period commencing from Customer’s notice

of nonconformity through the remainder of the Initial Term or Extension Term, as applicable.

9.2 Warranty Disclaimers.

EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH ABOVE, PROOFPOINT AND PROOFPOINT LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY WARRANTIES OF REGULATORY COMPLIANCE, PERFORMANCE, ACCURACY, RELIABILITY, AND NONINFRINGEMENT, TO THE EXTENT PERMITTED BY

APPLICABLE LAW. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT.

PROOFPOINT DOES NOT WARRANT: (I) THE ACCURACY OF THE INTENDED EMAIL BLOCKING OF ANY MAIL MESSAGE; (II) THAT EMAIL WILL NOT BE LOST; (III) THAT THE OPERATION OF THE PROOFPOINT PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE; (IV) THAT ALL SOFTWARE ERRORS WILL BE CORRECTED; OR (V) THAT THE PROOFPOINT PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS OR ATTACKS.

10. Limitation of Liability.

All consequential, incidental, special, punitive, exemplary, and indirect damages (including lost profits and loss of data) are disclaimed on behalf of Proofpoint (and Proofpoint is also required under its contracts with its suppliers and licensors to state in this Agreement that such suppliers and licensors also disclaim such damages herein). The foregoing exclusions/limitations of liability shall not apply (1) to personal injury or death caused by Proofpoint's negligence or fraud; (2) for express remedies requiring the specific type of relief under the law or these license terms; or (3) for any other matter for which liability cannot be excluded by law.

EXCEPT FOR (i) INTELLECTUAL PROPERTY INDEMNIFICATION OBLIGATIONS HEREIN, (ii) DAMAGES RESULTING FROM EITHER PARTY'S GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT, (iii) DAMAGES RESULTING FROM EITHER PARTY'S MATERIAL BREACH OF THE CONFIDENTIALITY SECTION, (iv) CUSTOMER'S BREACH OF THE CUSTOMER RESPONSIBILITIES SECTION, EACH PARTY'S AGGREGATE LIABILITY UNDER THE AGREEMENT FOR ANY CLAIMS, DAMAGES, OR LIABILITIES ("CLAIMS") SHALL IN NO EVENT EXCEED THE SUBSCRIPTION FEES PAID FOR THE APPLICABLE PROOFPOINT PRODUCT OVER THE PRECEDING TWELVE MONTHS FROM WHEN SUCH CLAIM AROSE.

11. Intellectual Property Rights.

11.1 Ownership. Customer retains all title, intellectual property and other ownership rights in all Customer Confidential Information, Customer Data and all data that Customer makes available for processing by the Proofpoint Products. Proofpoint retains all title, intellectual property and other ownership rights throughout the world in and to the Proofpoint Products, Documentation, and any work product and any modifications to, and derivative works of, the foregoing. Proofpoint hereby grants to Customer a non-exclusive, non- transferable, fully paid-up license to use any work product in connection with the Proofpoint Product licensed under the Agreement and solely for Customer's internal business purposes.

11.2 No Implied Rights. There are no implied rights and all rights not expressly granted herein are reserved. No license, right or interest in any Proofpoint trademark, copyright, patent, trade name or service mark is granted hereunder. Customer shall not remove from any full or partial copies made by Customer of the Software, Software Updates and Documentation any copyright or other proprietary notice contained in or on the original, as delivered to Customer.

11.3 Proofpoint Authorization and License. During the Term of the Agreement, Customer hereby (i) grants to Proofpoint and its service providers a worldwide, limited term license to collect and process certain Customer Confidential Information and Customer Data, and (ii) authorizes Proofpoint to collect and process certain Personal Data, for: (a) abuse, fraud and threat awareness, detection and prevention, (b) compliance, and (c) security purposes, in accordance with the Agreement. "Customer Data" means the Customer specific configurations and rules implemented in the Proofpoint Products, and any Customer

content processed by the Proofpoint Products (e.g., email text and attachments) that is not Personal Data.

Customer acknowledges and agrees that development of Threat Analytics from Proofpoint's ecosystem is critical to the functionality of the Proofpoint Products. Customer hereby authorizes Proofpoint to collect Threat Analytics during the Term of the Agreement. Further, Customer hereby authorizes Proofpoint to use Threat Analytics worldwide to build, enhance, improve and maintain Proofpoint services; provided that if Customer provides written legal notice to Proofpoint on or after expiration or termination of the applicable Proofpoint Services instructing Proofpoint to delete any Personal Data included in Threat Analytics, it will be deleted within 18 months of such notice. "Threat Analytics" means information collected, generated and/or analyzed by the Proofpoint Products such as log files, statistics, aggregated data and derivatives thereof.

12. Intellectual Property Rights Indemnification.

12.1 Proofpoint's Duty to Indemnify. Subject to the subsections below within this section, Proofpoint agrees to defend and indemnify Customer from and against any third-party claim filed against Customer alleging that the Proofpoint Product(s), as sold and delivered to Customer (the "Indemnified Products"), directly infringe the valid intellectual property rights of a third party (an "IP Claim"). Proofpoint agrees to pay and hold Customer harmless against any amounts finally awarded by a court having competent jurisdiction in respect of such IP Claim or pursuant to a settlement accepted by Proofpoint in writing. Proofpoint may, at its sole election and expense: (i) procure sufficient rights to allow Customer continued use of the Indemnified Products under the terms of the Agreement; (ii) replace or modify the Indemnified Products to avoid the alleged infringement; or (iii) if the foregoing options are not reasonably practicable, terminate Customer's rights to use the Indemnified Products and refund all amounts paid by Customer to Proofpoint attributable to Customers' future usage or access to the Indemnified Products.

12.2 Exclusions. Proofpoint shall have no obligation or any liability to Customer for any IP Claim arising out of or related to: (i) modifications or adaptations to the Indemnified Products made by Customer or Customer's agents; (ii) the use of the Indemnified Products in combination with any other product, service or device, if the IP Claim would have been avoided by the use of the Indemnified Products without such other product, service or device not provided by Proofpoint to Customer or Customer's agents; (iii) compliance with Customer's specific instructions for customization of an Indemnified Product made solely for or on behalf of Customer; (iv) use or exploitation of the Indemnified Products other than as set forth in the Agreement or applicable Documentation; or (v) Customer being given an update, modification, or replacement to an Indemnified Product by Proofpoint and failing to implement such update, modification, or replacement within a reasonable period of time.

12.3 Process. Proofpoint's obligations under this section are conditioned upon the following: (i) Customer first providing written notice of the IP Claim to Proofpoint within thirty (30) days after Customer becomes aware of or reasonably should have been aware of the IP Claim (provided, however, the failure to provide such notice will only relieve Proofpoint of its indemnity obligations hereunder to the extent Proofpoint is prejudiced thereby); (ii) Customer tendering control of the IP Claim to Proofpoint at the time Customer provides written notice of such IP Claim to Proofpoint; and (iii) Customer providing reasonable assistance, cooperation and required information with respect to defense and/or settlement of the IP Claim. Customer may at its sole expense participate in the IP Claim defense, except that Proofpoint will retain sole control of the defense and/or settlement, to the extent consistent with applicable State law. Proofpoint shall not agree to any settlement of an IP Claim that includes an injunction against Customer or admits Customer liability without Customer's prior written consent.

12.4 Exclusive Remedy. This section describes the sole and exclusive remedy of Customer and the entire liability of Proofpoint with respect to any IP Claim.

13. Term/Termination.

Upon expiration of the initial term and any extension term(s) under each Purchase Order, the Subscription Term applicable to such Purchase Order shall automatically renew for subsequent extension terms unless otherwise agreed by the parties or either party gives the other notice of non-renewal at least ninety (90) days prior to the end of the relevant Subscription Term.

Either party may terminate the Agreement or any Purchase Order (i) immediately upon written notice if the other party commits a non-remediable material breach; or (ii) if the other party fails to cure any remediable material breach within thirty (30) days of being of notified in writing of such breach.

On termination or expiration of the Agreement, all Software licenses, Service access, granted under the Agreement shall automatically terminate with immediate effect. In the event of the termination or expiration of the Agreement, the provisions of the Agreement which by their nature extend beyond the expiration or termination of the Agreement shall survive. Within thirty (30) days after expiration or termination of the License to use the Proofpoint Product, Customer shall: (i) certify in writing to Proofpoint that all copies of the Software, Software Updates, and Documentation in any form, including partial copies or extracts thereof, have been destroyed or returned to Proofpoint, and (ii) retrieve or dispose of Customer data from or within the Proofpoint Products and/or systems. Upon 30 days of termination of the License to use the Proofpoint Product, Customer data in the Proofpoint Product and/or systems may be rendered illegible, deleted or written over, including any back-up Customer data.

14. Miscellaneous.

A. Governing Law. This Agreement shall be governed by the law of the State where the Customer resides, exclusive of its choice of laws rules. The Uniform Computer Information Transaction Act shall not apply to this Agreement.

B. Force Majeure. Neither party shall be liable to the other for any delay or failure to perform hereunder due to circumstances beyond such party's reasonable control, including, acts of God, or the public enemy, acts of Government in its sovereign or contractual capacity, fires, floods, earthquakes, epidemics, quarantine restrictions, strikes, unusually severe weather and delays of common carriers, and other acts beyond a party’s reasonable control or possession including acts, civil unrest, acts of terror, strikes or other labor problems (excluding those involving such party's employees) or third-party service disruptions involving hardware, software or power systems and denial of service attacks.

C. Entire Agreement. This Agreement constitutes the entire agreement of the parties and supersedes all prior or contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No amendment or waiver of any provision of the Agreement shall be effective unless in writing and signed by the party against whom the amendment or waiver is to be asserted. Notwithstanding any language to the contrary therein, any Purchase Order issued by Customer or Reseller shall be deemed a convenient order and payment device only and no terms (other than product name, license quantity, price, Subscription Term, and billing contact) stated in any Purchase Order shall be incorporated into the Agreement, and all such other terms shall be void and of no effect.

D. Severability. If any clause of the Agreement shall be adjudged by any board, court or tribunal of competent jurisdiction to be invalid or unenforceable, such judgment shall not affect, impair or invalidate the remainder of the Agreement, which shall remain enforceable by the parties.

E. Open Source Software: Proofpoint Appliance/Software for Customer On-Site Deployment. Open Source Software may be a component of the Software provided to Customer for on-site deployment. Proofpoint is required by Open Source Software requirements to inform the end user of certain facts, including the following:

“Open Source Software" means various open source software, including GPL software which is software licensed under the GNU General Public License as published by the Free Software Foundation, and components licensed under the terms of applicable open source license agreements included in the materials relating to such software. Open Source Software is composed of individual software components, each of which has its own copyright and its own applicable license conditions. Customer may obtain information (including, if applicable, the source code) regarding the inclusion of Open Source Software in the Software by sending a request, with Customer’s name and address to Proofpoint at the address specified in the Order.

Customer may redistribute and/or modify the GPL software under the terms of the GPL. A copy of the GPL is included on the media on which Customer receives the Software or included in the files if the Software is electronically downloaded by Customer. This offer to obtain a copy of the source files for GPL software is valid for three (3) years from the date Customer acquired the Appliance Software.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L6 – Service Category 6: Content Delivery Network

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Cloudflare CDN

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 9. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 9 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 9 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-9 / 8) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: A Content Delivery Network (CDN) optimizes the delivery of web content by distributing it across a network of edge servers located globally. This reduces latency, improves page load times, and enhances the user experience, especially for content-heavy websites or applications. The Solution must ensure secure and efficient content delivery, while providing protection against common web-based attacks through mitigation of attacks such as distributed denial of service or web application exploits.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cloudflare's Content Delivery Network (CDN) provides comprehensive optimization and security through a globally distributed network of edge servers strategically positioned across 350+ cities worldwide. This extensive infrastructure enables efficient content delivery while maintaining robust protection against web-based threats.

Key features of our CDN solution include:

Content Optimization and Delivery:

●Intelligent caching mechanisms that store and serve content from servers closest to end-users

●Advanced content compression and minification to reduce file sizes

●HTTP/3 and QUIC protocol support for enhanced performance

●Smart routing technology that continuously monitors network conditions to select optimal paths

●Automated content optimization for images, scripts, and other web assets

●Browser cache revalidation to minimize unnecessary downloads

Performance Enhancement:

●Significant reduction in latency through edge computing capabilities

●Improved page load times through efficient content distribution

●Automatic mobile optimization for better user experience across devices

●Load balancing across multiple servers to handle traffic spikes

●Tiered cache architecture to maximize hit rates and minimize origin load

●Real-time performance analytics and monitoring

Security Features:

●Advanced DDoS mitigation protecting against volumetric attacks

●Web Application Firewall (WAF) with regular rule updates

●Bot management to identify and control automated traffic

●SSL/TLS encryption for secure content delivery

●Rate limiting to prevent abuse and maintain stability

- Real-time threat intelligence integration

Our CDN employs sophisticated caching strategies that:

- Automatically detect and cache static content
- Enable custom cache rules for different content types
- Provide instant cache purge capabilities globally
- Support dynamic content acceleration
- Allow granular control over cache behavior
- Maintain content freshness through configurable TTL values

The integrated security features protect against:

- Layer 3/4 DDoS attacks
- Application-layer attacks
- SQL injection attempts
- Cross-site scripting (XSS)
- Zero-day vulnerabilities
- Malicious bot activities

Performance Benefits:

- Up to 50% faster page load times
- Reduced bandwidth consumption
- Improved search engine rankings
- Enhanced user engagement
- Decreased server load
- Better mobile performance

The solution's architecture ensures:

- High availability through redundant systems
- Automatic failover capabilities
- Seamless scalability during traffic spikes
- Real-time performance monitoring
- Detailed analytics and reporting
- 24/7 expert support

This comprehensive approach to content delivery and security enables organizations to provide fast, reliable, and secure access to their web content while maintaining protection against evolving cyber threats. Our CDN continuously adapts to changing network conditions and security landscapes, ensuring optimal performance and protection for content-heavy websites and apps.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Distributed Edge Serve Architecture – Solution should allow content to be cached and served from the server closest to the end-user to reduce latency and improve performance.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare's distributed edge architecture caches and serves content from servers closest to end-users across 350+ global cities. This proximity-based approach minimizes data travel distance, significantly reducing latency and load times. The system's intelligent routing technology continuously monitors network conditions to select optimal paths, ensuring fast, reliable content delivery while reducing origin server load during peak traffic periods.

Prompt 3: Support for Dynamic Content Acceleration – Solution should optimize the delivery of personalized or frequently updated content through intelligent routing and caching mechanisms.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare optimizes dynamic content delivery through intelligent routing and advanced caching mechanisms. Argo Smart Routing analyzes network conditions in real-time to select the fastest paths, while tiered caching brings dynamic content closer to end-users. Features like Cache Key customization and personalized content caching ensure rapid delivery of frequently updated content while maintaining performance and content freshness.

Prompt 4: Content Caching Controls – Solution should allow administrators to define TTL (time-to-live) values, cache purging rules, and caching policies that align with the organization’s needs.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare provides comprehensive caching controls through an intuitive dashboard and API. Administrators can set custom Time-to-Live (TTL) values, implement immediate cache purging across global edge servers, and create specific caching policies for different content types. The platform enables granular control over which URLs, file types, and query strings are cached, ensuring flexible content management aligned with organizational requirements.

Prompt 5: Integrated DDoS Mitigation – Solution should protect web applications from volumetric attacks by filtering malicious traffic before it reaches the origin server.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare's DDoS mitigation system protects web applications by filtering malicious traffic at the edge before reaching origin servers. Cloudflare’s large-capacity network infrastructure absorbs and neutralizes volumetric attacks while analyzing traffic patterns to distinguish legitimate from malicious requests. This automated, always-on protection ensures continuous availability by blocking harmful traffic in real-time without manual intervention.

Prompt 6: Integration Web Application Firewall – Solution should protect web applications from exploits.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare's Web Application Firewall (WAF) protects against exploits through managed rule sets that automatically block OWASP Top 10 vulnerabilities, including SQL injection and XSS attacks. The system includes regularly updated proprietary rules for emerging threats, while allowing custom rule creation for specific security needs. Additional features include rate limiting and bot management to control traffic spikes and malicious automation.

Prompt 7: Real-Time Traffic Analytics – Solution should provide insights into website traffic, user behavior, cache hit/miss ratios, and security incidents such as DDoS attempts or SSL handshake failures

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare's analytics platform delivers comprehensive real-time insights through an intuitive dashboard, monitoring network performance, traffic patterns, and security events across distributed environments. The solution provides detailed visibility into user behavior, application usage, and threat activities through customizable reports and alerts. Administrators can track key metrics, analyze traffic trends, and identify security incidents with granular logging and visualization tools.

Prompt 8: Customizable Caching Rules – Solution should allow selective caching of specific content types (e.g., static images, JavaScript files, or video files) and exclusion of sensitive or dynamic data from the cache.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cloudflare provides granular caching controls allowing administrators to selectively cache specific content types while excluding sensitive data. Through Page Rules and Cache Keys, the platform enables customized caching behavior for different file types like images, JavaScript, and video files. Administrators can define caching rules based on URL patterns, HTTP headers, and cookies, ensuring fast delivery while maintaining data privacy.

Prompt 9: Integration of CTI Data Feeds – Solution should allow the CDN to identify and block traffic from known malicious IP addresses or domains, as well as protecting against emerging DDoS threats flagged by threat intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cloudflare's network learns from traffic that spans millions of Internet properties, enabling machine-learning based protection, behavioral analytics, and intelligent routing around problems in real-time from the following sources:

- Enriched data with feeds from premium third-party providers
- Threat data gathered from securing millions of Internet properties
- In Q3'24 Cloudflare blocked an average of 165 billion cyber threats each day
- 46 million HTTP requests per second

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Cloudflare is committed to ensuring the continuous availability of our services, and offers a 100% uptime Service Level Agreement for Enterprise customers. In the rare event of downtime, Enterprise Plan customers receive a credit against the monthly fee in proportion to the respective disruption and affected customer ratio. For details on our SLAs, including customer support response times, please see:

https://www.cloudflare.com/enterprise-support-sla/

Cloudflare services are subject to the Enterprise Subscription Terms of Service available at:

https://www.cloudflare.com/enterpriseterms/

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Cortex XSIAM

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: The Security Operations Platform (SOP) must integrate multiple security tools and technologies into a single unified platform, providing comprehensive visibility into an organization’s IT environment. The Solution should allow security teams to detect, investigate, and respond to threats in real-time, correlating data from across the infrastructure to provide a holistic view of security incidents.

Please describe how Respondent’s proposed Solution meets the above prompt in the field below.

Palo Alto Networks’ Cortex portfolio is the industry’s most comprehensive product suite for SecOps, empowering enterprises with the best-in-class detection, investigation, automation, and response capabilities.

Our Cortex Extended Security Intelligence and Automation Management (XSIAM) is the AI-driven SecOps platform for the modern SOC, that is AI-driven and automated to simplify SecOps, stop threats at scale, and accelerate incident remediation. XSIAM reduces risk and operational complexity by centralizing multiple products into a single, converged platform purpose-built for SecOps. This unified data lake enables security analysts to correlate events across the entire infrastructure.

Our Cortex portfolio addresses the need for a unified security operations platform by integrating multiple security tools and technologies into a cohesive ecosystem. This provides visibility into an organization’s IT environment and allows security teams to detect, investigate, and respond to threats in real-time.

Cortex XSOAR is a SOAR platform that combines case management, intelligent automation and orchestration, and interactive investigation to serve Cyber Protection Teams (CPTs) across the incident lifecycle and across entire security stacks. By integrating with a wide range of security tools, XSOAR streamlines incident response, reduces manual effort, and accelerates remediation.

Cortex XDR is an endpoint solution that integrates endpoint, network, and cloud data to detect, investigate, and respond to sophisticated cyber threats using behavioral analytics and ML. It provides visibility and advanced threat detection, enabling security teams to swiftly identify and mitigate potential risks. Its logging capabilities provide detailed forensic data, enabling thorough incident investigation and response.

Cortex Xpanse provides continuous visibility into an organization's attack surface, identifying and assessing external-facing assets and potential vulnerabilities. This proactive approach helps reduce attack surface and mitigate risks before they are exploited. Cortex Xpanse is an active ASM solution that helps organizations actively discover, learn, and respond to unknown risks in all connected systems and exposed services.

The seamless integration between XSIAM, XDR, XSOAR, and Xpanse empowers security teams with a comprehensive and unified security operations platform:

- Gain comprehensive visibility: Correlate data from across the entire IT environment.
- Detect and respond to threats in real time: Leverage advanced analytics, ML, and automation to identify and mitigate threats swiftly.

● Streamline security operations: Automate workflows, orchestrate responses, and reduce manual effort with integrated SOAR capabilities.

● Proactively manage the attack surface: Continuously discover and assess external-facing assets and vulnerabilities to reduce the attack surface.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Log Event Aggregation and Correlation – Solution should log event aggregation and correlation from various security devices (firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services) to identify patterns and indicators of compromise.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Cortex XSIAM centralizes log collection from a wide array of security devices. The platform utilizes its advanced SIEM capabilities to aggregate these logs in real-time, enabling the comprehensive collection of security event data across the entire IT infrastructure. XSIAM's powerful analytics engine then correlates this data to identify patterns and detect anomalies and suspicious activities.

Prompt 3: Automated Incident Response Workflows – Solution should allow security operations teams to optionally automate common tasks such as blocking IP addresses, isolating infected devices, or generating alerts for further investigation

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Cortex XSIAM automates incident response workflows with customizable playbooks. These playbooks enable security operations teams to automate common tasks, such as blocking malicious IP addresses, isolating infected devices, and generating alerts for further investigation. The platform ensures that security measures are consistently applied, improving the organization’s overall security posture and operational efficiency.

Prompt 4: Real-Time Threat Detection – Solution should be powered by machine learning models and behavioral analytics, capable of identifying zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Cortex XSIAM identifies zero-day attacks, insider threats, and anomalous activities deviating from the organization's baseline. The platform continuously ingests and analyzes vast amounts of data from across the IT environment, including endpoints, network traffic, cloud services, and many other sources. Machine learning algorithms process this data to establish a dynamic baseline of normal behavior for users, devices, and applications.

Prompt 5: Customizable Dashboards – Solution should have dashboards displaying real-time security metrics, providing visualizations of key performance indicators (KPIs) such as the number of incidents, time-to-respond, or threat severity.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM provides highly customizable dashboards that display real-time security metrics, offering visualizations of KPIs such as the number of incidents, MTTR, and threat severity. The platform comes with out-of-the-box dashboards and reports that are ready to use. XSIAM allows organizations to customize these dashboards and reports to fit their specific needs. Security teams can create tailored visualizations that align with operational and strategic priorities.

Prompt 6: Incident Management Capabilities – Solution should provide detailed incident tracking, ticketing integration, and root cause analysis, ensuring that all security events are fully documented and addressed.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM provides detailed incident tracking, seamless ticketing integration, and robust root cause analysis. The platform's incident tracking system ensures that all security events are meticulously documented, allowing security teams to maintain a comprehensive record of every incident. XSIAM integrates seamlessly with ITSM systems such as ServiceNow, automatically creating tickets for identified incidents and tracking their progress throughout to resolution.

Prompt 7: Integration with Threat Intelligence Platforms (TIPs)– Solution should enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM integrates seamlessly with TIPs to enrich security alerts with contextual information about current threat actors, malware campaigns, and IoCs. XSIAM ingests and correlates threat data from various TIPs, including both open-source and commercial intelligence feeds. XSIAM enhances security alerts by providing detailed contextual information, such as threat actor profiles, associated malware, and relevant IoCs.

Prompt 8: Integration of CTI Data Feeds – Solution should Allow for real-time enrichment of alerts, correlating incidents with known global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures), improving situational awareness and response times

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM enhances the integration of CTI data feeds, enabling real-time enrichment of alerts by correlating incidents with known global threat actor campaigns, IoCs, and TTPs. Enriched intelligence is then applied to security alerts, providing contextual information that links detected incidents to broader threat actor activities and known cyber threat patterns. By correlating incidents with global threat data, XSIAM significantly improves situational awareness.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Service-Level Agreement

All capitalized terms not defined herein shall have the same meaning as set forth in the Palo Alto Networks End User Agreement.

Cortex XSIAM, XDR, XSOAR, and Xpanse-hosted services shall be available 99.9% of the time, measured monthly, excluding scheduled maintenance. Further, any downtime resulting from outages of third-party connections or utilities or other reasons beyond the control of Palo Alto Networks will be excluded.

Customer's sole and exclusive remedy and the entire liability of Palo Alto Networks, in connection with Cortex product service availability, shall be to credit customer 2% of monthly service fees (downtime credit) for each breach. A breach is defined as a period of 60 consecutive minutes of downtime (delays in data log ingestion are not considered downtime). Downtime shall begin to accrue as soon as customer notifies Palo Alto Networks that the service is down and will continue to accrue until service is restored.

In order to receive downtime credit, customers must notify Palo Alto Networks within 24 hours of service unavailability by initiating a help desk ticket. Failure to provide such notice forfeits the right to receive downtime credit. Such credits may not be redeemed for cash and shall not exceed one (1) week of service fees in any one (1) calendar month. Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate service under this Service-Level Agreement.

Palo Alto Networks will provide technical support based on the Customer Success Plan purchased:

- Under the Standard Plan, technical support is available via the Customer Support Portal.
- Under the Premium Plan, technical support is also available as above and by phone 24 hours per day, 7 days per week.

Customers may initiate a help desk ticket via support.paloaltonetworks.com. Palo Alto Networks will use commercially reasonable efforts to respond as follows:

Severity Level 1: Service is down; critically affects customer production environment. No workaround available yet. Standard: less than/equal to 2 hours; Premium: less than/equal to 1 hour

Severity Level 2: Service is impaired; customer production up, but impacted. No workaround available yet. Standard: less than/equal to 4 hours; Premium: less than/equal to 2 hours

Severity Level 3: A service function has failed; customer production not affected Support is aware of the issue and a workaround is available. Standard: less than/equal to 12 hours; Premium: less than/equal to 4 hours

Severity Level 4: Non-critical issue. Does not impact customer business. Feature, information, documentation, how-to, and enhancement requests from customer. Standard: less than/equal to 48 hours; Premium: less than/equal to 8 business hours

More Information

To learn more about Palo Alto Networks Support offerings, visit paloaltonetworks.com/support or contact your local account manager. For product information, visit paloaltonetworks.com/products.

Why Palo Alto Networks?

Palo Alto Networks is committed to your success in preventing successful cyberattacks. Our award-winning services and support organization give you timely access to technical experts and on- line resources to ensure your business is protected. We take our responsibility for your success seriously and continuously strive to deliver an exceptional customer experience. Our entire services organization and Authorized Support Centers are there to ensure maximum uptime and streamlined operations.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“Agreement”) GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term “Product” is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose (“Evaluations”), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

“Affiliate” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Services.

“End User Data” means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

“Enterprise Program” means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

“Hardware” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“Product” means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

“Published Specifications” mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. “Software” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“Subscription(s)” means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according

to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer’s access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks’ Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks’ Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks’ and its suppliers’ sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Splunk Security Operations Platform

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: The Security Operations Platform (SOP) must integrate multiple security tools and technologies into a single unified platform, providing comprehensive visibility into an organization's IT environment. The Solution should allow security teams to detect, investigate, and respond to threats in real-time, correlating data from across the infrastructure to provide a holistic view of security incidents.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Splunk Enterprise, Enterprise Security, and SOAR (Mission Control) offer a robust, integrated platform that unifies security tools and technologies, providing a comprehensive view of an organization's IT environment. As a data aggregation hub, Splunk collects security data from various sources, including security devices, network appliances, servers, databases, and applications. This centralized collection is vital for effective analysis, consolidating information that might otherwise be siloed across different systems.

Once the data is collected, Splunk's powerful indexing and search capabilities make it searchable and actionable. Security teams can run complex queries across all data, detecting patterns, anomalies, and potential indicators of compromise (IoCs) that might be hidden in isolated tools. Real-time correlation of data from diverse sources helps identify sophisticated threats and vulnerabilities that span multiple infrastructure areas.

Splunk also includes advanced visualization tools with customizable dashboards, presenting security metrics, ongoing threats, compliance statuses, and operational health in real time. These visualizations allow teams to quickly assess security posture and make rapid decisions to respond to emerging threats.

To enhance security, Splunk leverages AI and machine learning (ML) through its Machine Learning Toolkit (MLTK), empowering security teams to apply machine learning algorithms to the collected data. This enables predictive analytics, identifying potential vulnerabilities before exploitation or detecting anomalous behaviors deviating from normal patterns. AI/ML capabilities automate responses to known threats and assist with proactive threat hunting, enabling teams to stay ahead of emerging risks.

Splunk integrates seamlessly with a wide range of security tools, including endpoint protection, identity management, and threat intelligence solutions. This interoperability ensures that Splunk serves as a central hub for security operations, unifying data from disparate systems and correlating security events for a holistic view. The unified platform empowers security teams to detect, investigate, and respond to threats in real time, improving situational awareness and enhancing the organization's ability to mitigate risks.

In summary, Splunk provides a comprehensive, unified platform that aggregates and correlates security data across the IT environment. With advanced search, visualization, AI/ML capabilities, and integration with other security tools, Splunk enables security teams to proactively detect, investigate, and respond to threats, offering a real-time and holistic view of security incidents.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Log Event Aggregation and Correlation – Solution should log event aggregation and correlation from various security devices (firewalls, IDS/IPS, endpoint detection tools, network devices, and cloud services) to identify patterns and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk provides a centralized platform for log aggregation and event correlation to monitor and respond to security threats across diverse infrastructures. It integrates data from sources like firewalls, IDS/IPS, and cloud services, supporting formats like JSON and Syslog. Splunk ES uses advanced correlation, machine learning, and threat intelligence for real-time insights, while Splunk SOAR automates incident response to improve security and efficiencyPrompt 2 Response Goes Here.

Prompt 3: Automated Incident Response Workflows – Solution should allow security operations teams to optionally automate common tasks such as blocking IP addresses, isolating infected devices, or generating alerts for further investigation

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk SOAR automates incident response workflows, integrating with Splunk Enterprise Security to enhance security operations. It offers customizable playbooks for tasks like blocking malicious IPs, isolating devices, and generating alerts. Workflows can be fully automated with optional human intervention. Automated enrichment improves alert context, boosting decision-making, and reducing response times to enhance efficiency and scalability.Prompt 3 Response Goes Here

Prompt 4: Real-Time Threat Detection – Solution should be powered by machine learning models and behavioral analytics, capable of identifying zero-day attacks, insider threats, and anomalous activities that deviate from the organization's baseline.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk offers real-time threat detection with machine learning and behavioral analytics. Its Enterprise Security (ES) platform identifies anomalies like zero-day attacks and insider threats by tracking user behavior. Risk-Based Alerting (RBA) prioritizes threats by risk scores, reducing alert fatigue. Splunk integrates threat intelligence to enrich data, while SOAR automates responses like isolating devices or blocking IPs, speeding response times.Prompt 4 Response Goes Here

Prompt 5: Customizable Dashboards – Solution should have dashboards displaying real-time security metrics, providing visualizations of key performance indicators (KPIs) such as the number of incidents, time-to-respond, or threat severity.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk provides fully customizable, real-time dashboards that offer the State of Florida's security team immediate visibility into key security metrics. With Splunk ES, dashboards display critical data like incident status, response times, and threat severity. Visualizations like graphs and heatmaps help identify trends and prioritize threats. Real-time updates and interactive features support quick investigations aenhancing decision-makingPrompt 5 Response Goes Here.

Prompt 6: Incident Management Capabilities – Solution should provide detailed incident tracking, ticketing integration, and root cause analysis, ensuring that all security events are fully documented and addressed.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk offers comprehensive incident management, streamlining security event tracking and resolution. Splunk ES tracks incidents from detection to resolution, integrates with ticketing platforms, and ensures standardized documentation. It supports root cause analysis by correlating events, preventing recurrence and improving future responses. These features enhance accountability, operational efficiency, and continuous improvement in security operations. Prompt 6 Response Goes Here

Prompt 7: Integration with Threat Intelligence Platforms (TIPs)– Solution should enrich security alerts with contextual information about current threat actors, malware campaigns, and indicators of compromise.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk integrates with Threat Intelligence Platforms (TIPs) to enrich security alerts with real-time context on threat actors, malware campaigns, and IOCs. By correlating threat intelligence feeds, Splunk identifies known malicious IPs, domains, and file hashes, helping teams prioritize responses and reduce false positives. This integration enhances detection, accelerates incident response, and empowers security teams to identify and mitigate threats effectively.Prompt 7 Response Goes Here

Prompt 8: Integration of CTI Data Feeds – Solution should Allow for real-time enrichment of alerts, correlating incidents with known global threat actor campaigns, IoCs, and TTPs (Tactics, Techniques, and Procedures), improving situational awareness and response times

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Splunk integrates with CTI data feeds to enrich alerts in real-time, correlating incidents with known global threat actor campaigns, IoCs, and TTPs from the MITRE ATT&CK framework. This enables security teams to identify and respond to emerging threats faster, providing contextual information on attack patterns. It improves situational awareness, reduces response times, and enhances threat detection and prioritization for more effective defense.Prompt 8 Response Goes Here

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Service Level Commitment

The Splunk Cloud Services will be available 100% of the time, as measured by Splunk over each calendar quarter of the Subscription Term, and subject to the exclusions set forth below (the “Service Level Commitment”).

A Splunk Cloud Service is considered available if the Customer is able to login to its Splunk Cloud Service account and initiate a search using Splunk Software.

Service Level Credit:

If Splunk fails to achieve the above Service Level Commitment for a Splunk Cloud Service, Customer may claim a credit for such Splunk Cloud Service as provided below, up to a maximum credit per calendar quarter equal to one month's Splunk Cloud Service subscription fees.

PERCENTAGE AVAILABILITY PER CALENDAR QUARTER	CREDIT
100	NO CREDIT
99.99-99.999	2 HOURS
99.9-99.99	4 HOURS
99.0-99.9	8 HOURS
95.0-99.0	1 DAY
0-95.0	1 MONTH

Exclusions

A Customer will not be entitled to a service credit if it is in breach of its Agreement with Splunk, including payment obligations. The Service Level Commitment does not apply to any downtime, suspension or termination of the applicable Splunk Cloud Service (or any Splunk Content or Splunk Software operating in connection with the Splunk Cloud Service) that results from:

- Account suspension or termination due to Customer's breach of the Agreement.

- Routine scheduled maintenance (Splunk's Maintenance Policy is available at https://www.splunk.com/en_us/legal/splunk-cloud-platform-maintenance-policy.html).

- Unscheduled, emergency maintenance or an emergency caused by factors outside Splunk's reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Content, Third Party Content or Internet Service Provider failures or delays.

- A Customer's equipment, software or other technology, or third-party equipment, software or technology (other than those which are under Splunk's control).

- Failures resulting from software or technology for which Splunk is not responsible under the Agreement.

- Customer's ability or inability to operate the Forwarder software is addressed by Splunk support services. For purposes of the Service Level Commitment, the Forwarder software is excluded from the calculation of the availability of the Splunk Cloud Services.

No Service Level Commitment is provided for free, proof-of-concept or unpaid trial services

Service Credit Claims.

To receive a service credit, a Customer must file a claim for such credit within five (5) days following the end of the calendar quarter in which the Service Level Commitment was not met for an applicable Splunk Cloud Service, by contacting Splunk at splunk-cloud-billing@splunk.com with a complete description of the downtime, how the Customer was adversely affected, and for how long. Splunk reserves the right to deny the service credit if the Customer does not qualify.

The service credit remedy set forth in this Service Level Schedule is the Customer's sole and exclusive remedy for the unavailability of any applicable Splunk Cloud Service.

*All capitalized terms not otherwise defined are as set forth in the Splunk Cloud Terms of Service.

Splunk General Terms > https://www.splunk.com/en_us/legal/splunk-general-terms.html

Last Updated: September 4, 2024

These Splunk General Terms (“General Terms”) between Splunk LLC, a Delaware limited liability company, with its office at 3098 Olsen Drive, San Jose, California 95128, USA (“Splunk” or “we” or “us” or “our”) and you (“Customer” or “you” or “your”) govern your acquisition, access to, and use of Splunk’s Offerings, regardless of how accessed or acquired, whether directly from us or from another Approved Source. By clicking on the appropriate button, or by downloading, installing, accessing, or using any Offering, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to these General Terms, or if you are not authorized to accept the General Terms on behalf of Customer, do not download, install, access, or use any Offering. The “Effective Date” of these General Terms is: (i) the date of Delivery; or (ii) the date you access or use the Offering in any way, whichever is earlier. Capitalized terms are defined in the Definitions section below.

1. Your Use Rights and Limits

- Your Use Rights. We grant you a non-exclusive, worldwide, non-transferable and non-sublicensable right, subject to your compliance with these General Terms and payment of applicable Fees, to use acquired Offerings only for your Internal Business Purpose during the Term, up to the Capacity, and, if applicable, in accordance with the Order (“Use Rights”). You have the right to make a reasonable number of copies of On-Premises Products for archival and back-up purposes.

- Limits on Your Use Rights. Except as expressly permitted in the Order, these General Terms or Documentation, your Use Rights exclude the right to, and you agree not to (nor allow any user or Third Party Provider to): (i) reverse engineer, decompile, disassemble or otherwise attempt to discover source code or underlying structures, ideas, protocols or algorithms of, or used by, any Offering; (ii) modify, translate or create derivative works based on any Offering; (iii) use an Offering to ingest, process, monitor, analyze or service the devices, systems, networks or application data of any third party; (iv) resell, sublicense, rent the use of, transfer or distribute any Offering; (v) access or use an Offering to analyze, test, characterize, inspect, or monitor its availability, performance, or functionality for competitive purposes; (vi) access or use an Offering to develop, test, troubleshoot, support, or market any software or service that competes with any Offering, or that integrates, interoperates with, or constitutes an extension of any Offering and that you use or intend to use for a commercial purpose; (vii) access or use any Offering in order to analyze, test, characterize, inspect, or monitor its source code or underlying structures, ideas, protocols, or algorithms it contains or uses; (viii) attempt to disable or circumvent any license key or other technological mechanisms or measures intended to prevent, limit or control use or copying of, or access to, Offerings; (ix) separately use any of the applicable features and functionalities of the Offerings with external applications or code not furnished by us or any data not processed by the Offering; (x) exceed the Capacity; or (xi) use any Offering in violation of any applicable laws and regulations (including but not limited to any applicable data protection and intellectual property laws). For clarity, each of the foregoing subsections imposes a separate and independent limit on your Use Rights.

- Splunk Extensions. Your Use Rights in Splunk Extensions are limited to your use solely in connection with the applicable Offering and subject to the same terms and conditions for that Offering, unless a Splunk Extension is expressly provided under an Open Source Software license that provides broader rights in that Splunk Extension than the Use Rights you have in the underlying Offering. Despite anything to the contrary in these General Terms, and unless otherwise required by law, Splunk Extensions (excluding Splunk Extensions designated by us as premium) are provided "AS-IS" without any indemnification or warranties. Support and service levels for Splunk Extensions are as set out in the Support Terms.

- Trial, Beta, Test and Similar Offerings

o Trials and Evaluations. We may make certain Trial Offerings available to you under these General Terms. After the Term for the Trial Offering expires, you may continue to use that Offering only subject to payment of applicable Fees.

o Beta Offerings. We may make certain Beta Offerings available to you under these General Terms. Your Use Rights in any Beta Offering are further limited to your use solely for internal testing and evaluation of that Beta Offering during the period specified with the Beta Offering, and if no period is specified, then for the earlier of one year from the Beta Offering start date or when that version of the Beta Offering becomes generally available. We may discontinue a Beta Offering at any time and may decide not to make a Beta Offering or any of its features or functionality generally available.

o Test and Development Offerings. For Offerings identified as "Test and Development" on the Order, your Use Rights are further limited to your use of those Offerings on a non-production system for non-production uses only, including product migration testing or pre-production staging, or testing new data sources, types, or use cases.

o Free Offerings. We may make certain Offerings available for full use (i.e., not subject to limited evaluation purposes) at no charge under these General Terms. These free Offerings may have limited features, functions, and other technical Use Rights limitations.

o Limitations and Termination. Despite anything to the contrary in these General Terms, and unless otherwise stated in the Order or required by law, Trial Offerings, Beta Offerings, Test and Development and any free Offerings are provided "AS-IS" without any indemnification, warranties, maintenance, support or service level commitments. Unless otherwise stated in the Order, we reserve the right to terminate any Offering in this section 1.4 at any time without prior notice and without any liability.

- Specific Offering Terms. Specific security controls and certifications, data policies, service descriptions, Service Level Schedules and other terms specific to Offerings (“Specific Offering Terms”) are at http://www.splunk.com/SpecificTerms (which are incorporated by reference). We may change the Specific Offering Terms at any time and without notice, provided these changes will only apply to the Offerings ordered or renewed after the date of the change.

- Interoperability Requirements. If required by law, we will promptly provide the information you request to achieve interoperability between applicable Offerings and another independently created program on terms that reasonably protect our proprietary interests.

2. Purchasing Through Approved Sources

- Splunk Affiliate Distributors. We have appointed certain Splunk Affiliates as our non-exclusive distributors of the Offerings (each, a “Splunk Affiliate Distributor”). Each Splunk Affiliate Distributor is authorized by us to negotiate and enter into Orders with customers. Where a purchase is offered by a Splunk Affiliate Distributor, you will order from, and make payments to, that Splunk Affiliate Distributor. Each Order will be deemed a separate contract between you and the relevant Splunk Affiliate Distributor and will be subject to these General Terms. You agree that: (i) Splunk’s total liability under these General Terms as set out in section 20 (Limitation of Liability) states the overall combined liability of Splunk and our Splunk Affiliate Distributors; (ii) entering into Orders by a Splunk Affiliate Distributor will not be deemed to expand Splunk and its Affiliates’ overall responsibilities or liability under these General Terms; and (iii) you will have no right to recover more than once from the same event. We agree that: (a) the Splunk Affiliate Distributor will be liable for the performance of the Order; and (b) to the extent that any obligations of the Order are to be performed by us, the Splunk Affiliate Distributor will be responsible for, and ensure our compliance with, the terms of the Order.

- Approved Sources. These General Terms will govern any Offering that you acquire through any Approved Source. Your payment obligations (if any) will be with the Approved Source through whom you acquired the Offering. However, a breach of your payment obligations with any Approved Source for any Offering will be deemed to be a material breach of these General Terms between you and Splunk. In addition, if you fail to pay a Digital Marketplace for an Offering, we retain the right to enforce your payment obligations and collect directly from you. Any terms agreed between you and an Approved Source (other than us or a Splunk Affiliate Distributor) that are in addition to these General Terms are solely between you and that Approved Source. No agreement between you and that Approved Source is binding on us or will have any force or effect with respect to the rights in, or the operation, use or provision of, any Offering.

3. Your Third Party Providers

You may permit your Third Party Providers to access and use the Offerings on your behalf, provided that: (i) such access and use will at all times be subject to these General Terms and any applicable Order; (ii) you will ensure these Third Party Providers comply with these General Terms and any applicable Order; (iii) you are liable for any action or omission of any Third Party Provider if that action or omission would constitute a breach of these General Terms or any Order if done by you; and (iv) the aggregate use by you and all of your Third Party Providers must not exceed the Capacity.

4. Hosted Services

- Service Levels. When you purchase Hosted Services, we will make the applicable Hosted Services available to you during the Term in accordance with these General Terms. The Service Level Schedule in the Specific Offering Terms and associated remedies will apply to the availability and uptime of the applicable Hosted Service. If applicable, service credits will be available for downtime in accordance with the Service Level Schedule.

- Your Responsibility for Data Protection. You are responsible for: (i) selecting from the security configurations and security options made available by Splunk in connection with a Hosted Service; (ii) taking additional measures outside of the Hosted Service to the extent the Hosted Service does not provide the controls that may be required or desired by you; and (iii) routine archiving and backing up of Customer Content. You agree to notify Splunk promptly if you believe that an unauthorized third party may be using your accounts or if your account information is lost or stolen.

- Return of Customer Content. You may retrieve and remove Customer Content from the Hosted Services at any time during the Term. We will also make the Customer Content available for your retrieval for 30 days after termination of your subscription. After those 30 days, we will delete all remaining Customer Content without undue delay, unless legally prohibited. If you require assistance in connection with migration of Customer Content, we may require a mutually agreed upon fee for it.

5. Data Protection

We will follow globally recognized data protection principles for the processing of personal data as described in the applicable data processing addendum at https://www.splunk.com/en_us/legal/splunk-dpa.html (which is incorporated by reference). If we have separately executed a data processing addendum between us covering the same scope, it will apply instead of any data processing addendum posted online.

6. Security

- Security Program. We have implemented and will maintain an industry standard security program to protect our Offerings, IT systems, facilities and assets, and any Customer Confidential Information accessed or processed therein, including Customer Content in a Hosted Service and customer account information. Our Hosted Service security controls include commercially reasonable administrative, technical, and organizational safeguards designed to protect Customer Content against destruction, loss, alteration, unauthorized disclosure, or unauthorized access, such as threat and vulnerability management, incident response and breach notification procedures, disaster recovery plans, open source security scans, virus detection, industry-standard secure software development practices, and internal and external penetration testing in the development environment. Our general corporate security controls include information security policies and procedures, security awareness training, physical and environmental access controls, and vendor risk management.

- Security Exhibits. The specific security measures applicable to certain Offerings are described in the security exhibits at https://www.splunk.com/en_us/legal/splunk-security-addenda.html.

- Maintaining Protections. Despite anything to the contrary in these General Terms or any policy or terms referenced in these General Terms via hyperlink, we may update Security Exhibits from time to time, provided those updates do not materially diminish the overall security protections set out in these General Terms, applicable Specific Offering Terms or Security Exhibits.

7. Support and Maintenance

The specific Support Program included with an Offering will be identified in the Order. We will provide the purchased level of support and maintenance services for an Offering in accordance with the Support Terms effective on the Delivery of that Offering.

8. Configuration and Implementation Services

We offer additional services to configure and implement your Offering ("C&I Services"). These C&I Services are purchased under a Statement of Work and are subject to payment of applicable Fees. We provide C&I Services in accordance with our standard C&I Services terms at https://www.splunk.com/en_us/legal/professional-services-agreement.html, effective on the start date of the Statement of Work.

9. Our Compliance, Ethics and Corporate Responsibility

- Compliance. We will comply with the laws and regulations applicable to our business and the provision of the Offerings to our customers generally, and without regard to your particular use of the Offering.

- Ethics and Corporate Responsibility. We are committed to acting ethically and in compliance with applicable law, and we have policies and guidelines in place to provide awareness of, and compliance with, the laws and regulations that apply to our business globally. We are committed to ethical business conduct, and we use diligent efforts to perform in accordance with the highest global ethical principles, as described in the Splunk Code of Business Conduct and Ethics at https://www.splunk.com/en_us/pdfs/legal/code-of-business-conduct-and-ethics.pdf.

- Anti-Corruption. We implement and maintain programs for compliance with applicable anti-corruption and anti-bribery laws. Our policy prohibits offering or soliciting any illegal or improper bribe, kickback, payment, gift, or thing of value to or from any of your employees or agents in connection with these General Terms. If we learn of any violation of the above, we will use reasonable efforts to promptly notify you at the main contact address that you have provided to us.

- Export. We certify that we are not on any of the relevant U.S. or EU government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. Export information regarding our Offerings, including our export control classifications for our Offerings, is at https://www.splunk.com/en_us/legal/export-controls.html.

- Environmental, Social and Governance. Our positions and commitments on environmental, social and governance aspects of our business, including our Global Impact Reports and ESG Position Statement, are in our ESG Resource Center at https://www.splunk.com/en_us/global-impact/esg-resources.html.

10. Usage Data

We collect and process Usage Data as set out in Splunk's Privacy Statement at https://www.splunk.com/en_us/legal/privacy/privacy-policy.html. Usage Data does not include Customer Content and will be kept confidential.

11. Capacity and Usage Verification

- Certification and Verification. Upon our request, you will provide us with a certification signed by your authorized representative verifying that your use of the Offering is in accordance with these General Terms and any applicable Order. For On-Premises Products, we may also ask you from time to time, but not more frequently than once every 12 months, to cooperate with us to verify usage and adherence to the Capacity. If we request such a verification, you agree to provide us reasonable access to the On-Premises Product installed at your facility (or as hosted by your Third-Party Provider). If we do any verification, it will be performed with as little interference as possible to your use of the On-Premises Product and your business operations. We will comply with your (or your Third-Party Providers') reasonable security procedures.

- Overages. If a verification or usage report reveals that you have exceeded the Capacity or Use Rights, then we will have the right to invoice you using the applicable Fees at list price then in effect, which will be payable in accordance with these General Terms. Except where you have paid the applicable Approved Source for such additional Capacity or Use Rights, we will have the right to directly invoice you for overages, regardless of whether you acquired the Offering from us or another Approved Source.

12. Our Use of Open Source

Certain Offerings may contain Open Source Software. In the applicable Documentation, we make available a list of Open Source Software and applicable licenses incorporated in our On-Premises Products to the extent required by the respective Open Source Software licenses. Any Open Source Software that is delivered as part of your Offering and which may not be removed or used separately from the Offering is covered by the warranty, support and indemnification provisions applicable to the Offering, but only to the extent that Open Source Software is used as intended with the Offering. Some of the Open Source Software may have additional terms that apply to the use of the Offering (e.g., the obligation for us to provide attribution of the specific licensor), and those terms will be included in the Documentation. However, those terms will not: (i) impose any additional restrictions on your use of the Offering; or (ii) negate or amend our responsibilities with respect to the Offering.

13. Third Party Extensions, Content and Products

- Third Party Extensions on Splunkbase. We may make Third Party Extensions available from Splunkbase. We do not represent, warrant or guarantee the accuracy, integrity, quality, or security of any Third Party Extension, even if that Third Party Extension is identified as “certified” or “validated” for use with the Offering. Your use of a Third Party Extension may be subject to additional terms, conditions or policies. We may block or disable access to a Third Party Extension at any time.

- Third Party Content. Hosted Services may contain features that enable interoperation with Third Party Content that you choose to add to a Hosted Service. You may be required to: (i) separately obtain access to Third Party Content from its provider; and (ii) grant us access to your accounts with those providers. By choosing to enable such interoperation by allowing us to enable access to Third Party Content, you: (a) certify that you are authorized to do so; and (b) authorize us to allow that provider to access Customer Content as necessary for interoperation. We are not responsible or liable for disclosure, modification or deletion of Customer Content resulting from such interoperation, nor are we liable for damages or downtime or other impact on the Hosted Service, resulting directly or indirectly from your use of or reliance on Third Party Content, sites or resources.

- Splunk as a Reseller. When you purchase third party products ("Third Party Products") from us as specified in an Order (which products will include third party software, but not any support which we have contracted to provide), the following applies. We act solely as a reseller of Third Party Products, which are fulfilled by the relevant third party vendor, and purchase and use of Third Party Products is subject solely to the terms, conditions and policies made available by that third party vendor. Consequently, we make no representation or warranty of any kind regarding the Third Party Products, whether express, implied, statutory or otherwise, and specifically disclaim all implied terms, conditions and warranties (including as to quality, performance, availability, fitness for a particular purpose or non-infringement) to the maximum extent permitted by applicable law. You will bring any claim in relation to Third Party Products against the applicable third party vendor directly. In no event will we be liable to you for any claim, loss or damage arising out of the use, operation or availability of any Third Party Product (whether such liability arises in contract, negligence, tort, or otherwise).

14. Your Compliance

- Lawful Use of Offerings.When you access and use an Offering, you are responsible for complying with all laws, rules, and regulations applicable to your access and use. This includes, without limitation, being responsible for your Customer Content and users, their compliance with these General Terms, how you acquired your Customer Content, and the accuracy and lawful use of your Customer Content.

- PHI, PCI Data and ITAR Data. You may not transmit or store PHI, PCI Data or ITAR Data within a Hosted Services unless you have specifically acquired an Offering for that applicable regulated Hosted Services environment.

- Registration. You agree to provide accurate and complete information when you register for and use an Offering and agree to keep this information current. Each person who uses an Offering must have a separate username and password. For Hosted Services, you must provide a valid email address for each person authorized to use your Hosted Services. We may require additional information for certain Offerings (e.g., technical information necessary for your connection to a Hosted Service), and you will provide this information as we reasonably request. You are responsible for securing, protecting, and maintaining the confidentiality of your account usernames, passwords and access tokens.

- Export Compliance. You will comply with all applicable export laws and regulations of the United States (which apply irrespective of the use location of the Offerings) and any other country ("Export Laws") where your users use any of the Offerings. You certify that you are not on any of the relevant U.S. government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. You will not export, re-export, ship, transfer or otherwise use the Offerings in any country subject to an embargo or other sanction by the United States, including, without limitation, Iran, Syria, Cuba, the Crimea Region of Ukraine, Sudan and North Korea, and you will not use any Offering for any purpose prohibited by the Export Laws.

- Acceptable Use. For any Hosted Services, you will also abide by our Hosted Services Acceptable Use Policy at https://www.splunk.com/view/SP-CAAAMB6.

- GovCloud Services. This section 14.6 will apply to you if you access or use any Hosted Services in the specially isolated AWS GovCloud (U.S.) region (including without limitation any Hosted Services that are provisioned in a FedRAMP authorized environment within the AWS GovCloud (U.S.) region)). You hereby represent and warrant that: (i) you are a "U.S. Person" as defined under ITAR (see 22 CFR part 120.62); (ii) you have and will maintain a valid Directorate of Defense Trade Controls registration, if required by ITAR; (iii) you and your end users are not subject to export control restrictions under U.S. export control laws and regulations (i.e., users are not denied or debarred parties or otherwise subject to sanctions); (iv) you will maintain an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including ITAR, as applicable; and (v) you will maintain effective access controls as described in the Specific Offering Terms for the applicable Hosted Services. You are responsible for verifying that any user accessing Customer Content in the Hosted Services in the AWS GovCloud (U.S.) region is eligible to access such Customer Content. The Hosted Services in the AWS GovCloud (U.S.) region may not be used to process or store classified data. You will be responsible for all sanitization costs incurred by us if users introduce classified data into the Hosted Services in the AWS GovCloud (U.S.) region. You may be required to execute additional addenda to these General Terms before provisioning of selected Hosted Services.

15. Confidentiality

- Confidential Information. Each party will protect the Confidential Information of the other. Accordingly, receiving party agrees to: (i) protect disclosing party's Confidential Information using the same degree of care (but in no event less than reasonable care) that it uses to protect its own Confidential Information of a similar nature; (ii) limit use of disclosing party's Confidential Information to only for purposes consistent with these General Terms; and (iii) use commercially reasonable efforts to limit access to disclosing party's Confidential Information to its employees, contractors, agents, or Affiliates, each of which has a bona fide need to access such Confidential Information for purposes consistent with these General Terms, and who are subject to confidentiality obligations no less stringent than those set out here.

- Compelled Disclosure of Confidential Information. Despite the provisions above, receiving party may disclose Confidential Information of disclosing party if it is compelled by law enforcement agencies or regulators to do so, provided receiving party gives disclosing party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at disclosing party's cost, if disclosing party wishes to contest the disclosure. If receiving party is compelled to disclose disclosing party's Confidential Information as part of a civil proceeding to which disclosing party is a party, and disclosing party is not contesting the disclosure, disclosing party will reimburse receiving party for its reasonable cost of compiling and providing secure access to such Confidential Information.

16. Payment

- Payment Terms. The payment terms in this section 16 only apply when you purchase Offerings directly from us.

- Fees. You agree to pay all Fees specified in the Orders. Fees are non-cancelable and non-refundable, except as otherwise expressly stated in these General Terms. Without limiting any of our other rights or remedies, overdue charges may accrue interest monthly at the rate of 1.5% of the then-outstanding unpaid balance, or the maximum rate permitted by law, whichever is lower. Fees are due and payable either within 30 days from the date of our invoice or as otherwise stated in the Order.

- Credit Cards. For e-commerce transactions, if you choose to pay by credit or debit card, then you: (i) will provide us or our designated third party payment processor with valid credit or debit card information; and (ii) authorize us or our designated third party payment processor to charge such credit or debit card for all items listed in the applicable Order. Such charges must be paid in advance or in accordance with any different billing frequency stated in the applicable Order. You are responsible for providing complete and accurate billing and contact information and notifying us in a timely manner of any changes to such information.

- Taxes.Fees are exclusive of applicable taxes and duties, including any applicable sales and use tax. You are responsible for paying any taxes or similar government assessments (including, without limitation, value-added, sales, use or withholding taxes). We will be solely responsible for taxes assessable against us based on our net income, property, and employees.

17. Warranties

- Relationship to Applicable Law. You may have legal rights in your country that prohibit or restrict the limitations set out in this section 17, which applies only to the extent permitted under applicable law.

- General Corporate Warranty. Each party warrants that it has the legal power and authority to enter into these General Terms.

- Hosted Services Warranty. We warrant that during the Term: (i) we will not materially decrease the overall functionality of the Hosted Services; and (ii) the Hosted Services will perform materially in accordance with the Documentation. For any breach of these warranties, our entire liability, and your sole remedy, will be for us to: (a) modify or correct the Hosted Service so that it conforms to the foregoing warranty; or (b) if we determine that (a) is not commercially, technically or operationally reasonable, terminate the non-conforming Hosted Service, and refund to you any prepaid but unused Fees for the remainder of the Term.

- On-Premises Product Warranty. We warrant that for a period of 90 days from its Delivery, the On-Premises Product will substantially perform the material functions described in the Documentation, when used in accordance with the Documentation. For any breach of this warranty, our entire liability, and your sole remedy, will be for us to: (i) modify, or provide an Enhancement for, the On-Premises Product so that it conforms to the foregoing warranty; (ii) replace your copy of the On-Premises Product with a copy that conforms to the foregoing warranty; or (iii) if we determine that (i) or (ii) is not commercially, technically or operationally reasonable, terminate the Offering with respect to the non-conforming On-Premises Product and refund to you the Fees paid for such non-conforming On-Premises Product.

- Disclaimer of Implied Warranties. Except as expressly set out above, and to the extent allowed by law, the Offerings are provided “AS IS” with no other warranties or representations whatsoever express or implied. We and our suppliers and licensors disclaim all warranties and representations not expressly set out above, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, noninfringement, or quiet enjoyment, and any warranties arising out of course of dealing or trade usage. We do not warrant that use of Offerings will be uninterrupted, error free or secure, or that all defects will be corrected.

18. Ownership

- Offerings. As between you and us, we own and reserve all right, title, and interest in and to the Offerings and other Splunk materials, including all Intellectual Property Rights therein. We retain rights in anything delivered or developed by us or on our behalf under these General Terms. No rights are granted to you other than as expressly set out in these General Terms.

- Customer Content. You own and reserve all right, title and interest in your Customer Content. By sending Customer Content to a Hosted Service, you grant us a worldwide, royalty free, non-exclusive license to access and use the Customer Content for purposes of providing you the Hosted Service and as set out in the Specific Offering Terms. Subject to section 18.1, you own any reporting results that you or your Third Party Providers may derive from Customer Content through the use of the Offerings.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L8 – Service Category 8: Identity and Access Management (IAM)

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Okta Identity and Access Management (IAM) and Privileged Access Management

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: IAM Solutions must provide centralized management for digital identities and control access to systems and data based on organizational policies. The Solution should manage the full lifecycle of user identities, from onboarding to de-provisioning, and enforce access control through role-based (RBAC) and attribute-based (ABAC) mechanisms.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Okta Fine Grained Authorization (Okta FGA) provides a cloud-native, centralized, and API-driven approach to managing complex authorization requirements that is flexible and scalable. Okta's centralized view into authorization policies allows customers to manage their compliance goals efficiently.

Authorization as a service eliminates authorization complexity across systems, users, and applications and delivers scalable and fully flexible authorization: customers can use Okta FGA to build team collaboration, multi-tenancy, custom roles, IoT, and cloud entitlement management. Okta distinguishes itself with a cloud-native, centralized authorization as a service that speeds time-to-value by making it easier and faster for developers to build superior customer experiences, innovate rapidly, and scale their business.

Okta Lifecycle Management centralizes and automates lifecycle management across all apps on-premise and in the cloud. Users and their devices get instant access to the applications they need, for not a minute longer than they need, while the IT team saves significant management costs.

Lifecycle Management collects all information about a user, including their job title, the groups they belong to, which devices they own, and more from AD, HR, CRM, or ERP systems. Most importantly, the directory is lifecycle aware— a user can be staged, activated, suspended, deactivated, and deleted, based on lifecycle state change events. IT teams can create a self-service flow that sends an app access request directly to the application business owner, like a Sales Director managing Salesforce, who has the best idea of what access level is appropriate. The ticket never touches the IT helpdesk. The following features and capabilities are possible with LCM: Group Membership Rules, App-as-Source, Attribute-Level Sourcing, Access Request Workflow, Okta Provisioning Agent, and Access Reports.

Okta fully supports RBAC and ABAC, which can be configured by defining Okta Groups with roles as well as through more advanced features such as Okta Lifecycle Management, Okta Privileged Access, Okta Workflows, and Okta Hooks. Rules can be created that auto populate users to certain Role Groups, which then automatically provisions them to applications assigned to that role. Groups are commonly used to assign SSO access within Okta and to provision users to apps with specific entitlements (roles, profiles, etc). When rules are configured to populate groups based on attributes, you achieve ABAC and RBAC.

Okta can also empower ABAC and RBAC within the downstream applications it is authenticating access to. Okta allows admins to customize the attributes passed back to the applications in the SAML assertions or OIDC ID Tokens. These custom attributes can then be utilized by the application in question to customize the experience of the user based on attributes contained in the user's profile within Okta.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Single Sign-On (SSO) – Solution should be compatible across on-premise and cloud based applications, reducing password fatigue and ensuring a seamless login experience for users.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

SSO is part of a complete identity and access management solution for organizations accelerating their adoption of cloud and mobile apps. It enables your employees, contractors, and customers to securely access all your cloud and on-premises applications from anywhere and with any device.

SSO is supported across cloud-based and on-premise applications using pre-defined and Okta-maintained integrations, enabling IT to manage people, applications, and policies through one comprehensive service.

Prompt 3: Multi-Factor Authentication (MFA) – Solution should provide enforcement, supporting various authentication methods (e.g., Time-based one-time Password (TOTP), Short Message Service (SMS), biometrics) to add an extra layer of security.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Okta's native multi-factor options can be centrally administered in an integrated fashion. Admins can assign MFA to users based on group membership or application access. Any factor can be used for passwordless authentication. Built-in authenticators: Okta Verify OTP (soft token) on iOS, Android; Okta Verify w/ Push (soft token, app registration/certificate) on iOS, Android; Okta FastPass (MacOS, Windows, iOS, Android); SMS, Voice, WebAuthn, Yubikey, Smartcard/certificate, and risk checks.

Prompt 4: Role-Based Access Control (RBAC) and Attribute-Based Control (ABAC) – Solution should include mechanisms, enabling fine-grained access permissions based on user roles or attributes such as location, department, or security clearance.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Okta fully supports RBAC and ABAC, which can be configured by defining Okta Groups with roles as well as through more advanced features such as Okta Lifecycle Management, Okta Privileged Access, Okta Workflows, and Okta Hooks. Rules can be created that auto populate users to certain Role Groups, which then automatically provisions them to applications assigned to that role. When rules are configured to populate groups based on attributes, you achieve ABAC and RBAC.

Prompt 5: Federated Identity Management – Solution should allow cross-domain authentication using standard protocols like SAML, OAuth, and OpenID Connect.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Okta supports the following protocols/standards and more:

- Federation Identity Standards: SAML (1.1 and 2.0), WS-Fed, and OpenID Connect.
- Delegated Authorization: OAuth 2.0
- User Provisioning: SCIM 1.1 and 2.0
- Authentication / MFA Standards: AD, LDAP, WCP, RADIUS, FIDO U2F, FIDO2 WebAuthN, HTTP Headers, Kerberos, TOTP
- Form fill credential vault using Okta's Secure Web Authentication (SWA)
- Authorization Policy Engine: OPA
- Privileged Access: SSH, RDP
- Transport Security: HTTPS, TLS

Prompt 6: Privileged Access Management (PAM) – Solution should provide capabilities to control and monitor the use of administrative or high-privilege accounts, ensuring that elevated access is limited and auditable.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Okta Privileged Access empowers teams to gain visibility, meet compliance, and enforce zero-standing privileges. Okta Privileged Access is cloud-architected and integrated with Okta's workforce identity solution providing a single platform for IAM and PAM admins ease of use. OPA ensures passwordless, zero-trust access to critical roles, providing just-in-time access and securing privileged credentials, including local admin accounts, via Okta's modern cloud vault.

Prompt 7: Self-Service Functionality – Solution should allow users to manage their own passwords, request access to systems, and track the status of access requests through an approval workflow.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Okta manages entitlements via individual or group assignment, defining automatic (i.e. birthright apps) and those that can be requested. Okta Lifecycle Management provides entitlements based on onboarding/offboarding and app attributes. Okta Access Requests enables self-service approval workflows via the Access Request Portal or integrated apps (e.g., Slack, MS Teams).

Users can add/remove personal apps, add pre-approved corporate apps, and request apps with configured access request workflows.

Prompt 8: Integration of CTI Data Feeds – Solution should allow the IAM system to detect compromised credentials, suspicious login attempts, or help identify identity-related threat actor activities in real-time.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Okta provides service-level threat protection via Okta ThreatInsight, using static rules and machine learning to observe and derive intelligence from credential-based attacks. IP addresses creating password spray and brute force attacks across all customers are identified and put into the ThreatInsight pool, so admins can block or audit them in their org. Identity Threat Protection with Okta AI incorporates third-party signals from cybersecurity vendors to automate threat remediation.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Any Applicable SLA Goes Here

Okta Support makes every possible effort to respond to support incidents in accordance with the time frames defined in the Support Service Level Agreement (SLA).

Per Okta's MSA, initial response times and follow-up response times vary based on the Customer Success Package a customer has purchased and the Customer Support Ticket Severity / Priority Definition.

Okta's service platform is managed and maintained without any maintenance windows. Okta's standard support services are detailed here: https://www.okta.com/support-terms/

Okta's MSA is available here: https://www.okta.com/agreements

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L10 – Service Category 10: Secure Access Service Edge (SASE)

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Prisma Access

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8 Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for the proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Score for Prompts 2-9 / 8) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: SASE Solutions combine networking and security services, delivering both through a cloud-based framework that supports remote users, branch offices, and cloud applications. The Solution integrates Software-Defined Wide Area Networking (SD-WAN) with advanced security features like Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS).

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Palo Alto Networks Prisma Access addresses the requirements of a Secure Access Service Edge (SASE) solution:

● Cloud-Based Framework for Networking and Security:

○ Prisma Access is a cloud-delivered service that integrates network security, SD-WAN, and Autonomous Digital Experience Management (ADEM) into a single, unified platform. This architecture provides scalable, consistent security and connectivity across distributed environments, supporting remote users, branch offices, and cloud applications.

● Software-Defined Wide Area Networking (SD-WAN):

○ Prisma SD-WAN integrates with Prisma Access to deliver next-generation SD-WAN capabilities. This integration allows for intelligent traffic routing, application-aware policies, and optimization of bandwidth across various transport types. It enables secure and efficient connectivity for branch offices by leveraging the cloud for scalability and reducing the need for expensive traditional WAN infrastructure.

● Secure Web Gateway (SWG):

○ Prisma Access includes a Cloud SWG that safeguards access to the internet and cloud applications. It employs AI and machine learning for threat detection, supports deep visibility into encrypted traffic, and offers protection against web-based threats. This component helps in preventing data loss, credential theft, and ensures safe web usage.

● Cloud Access Security Broker (CASB):

○ The Next-Generation CASB within Prisma Access provides comprehensive control over SaaS applications. It offers visibility into usage, real-time data protection, and ensures compliance by applying security policies to both sanctioned and unsanctioned cloud applications.

● Zero Trust Network Access (ZTNA):

○ ZTNA 2.0 in Prisma Access provides least-privilege access based on continuous verification of trust, focusing on user identity, device posture, and application context rather than network location. It reduces the attack surface by employing fine-grained access controls, ensuring users only access what they need, when they need it, enhancing security while maintaining user experience.

● Firewall as a Service (FWaaS):

○ Through Prisma Access, FWaaS applies consistent security policies across all traffic, regardless of origin or destination, providing protection against threats with features like intrusion prevention, URL filtering, and application control. This service extends firewall protection to all edges of the network, including remote users and branches.

Prisma Access ensures these capabilities are managed via a unified policy framework, allowing for consistent security enforcement across all components. This holistic approach not only simplifies management but also enhances security by providing a single point of control and visibility. The solution's cloud-native architecture supports scalability and can adapt to the evolving needs of modern enterprises, making it apt for organizations adopting a hybrid work model or expanding their cloud usage.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: SD-WAN with Policy-Based Routing– Solution should enable dynamic, intelligent path selection to ensure optimal network performance for applications, even across distributed cloud environments.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Prisma SD-WAN dynamically selects optimal paths based on real-time SLAs, ensuring application performance. It integrates application-aware traffic engineering, supports multiple transports, and offers centralized management for policy-based routing across cloud environments.

Prompt 3: Zero Trust Network Access (ZTNA) Principles – Solution should enforce least-privilege access to applications based on identity and context (e.g., user role, device health, location) rather than assuming trust based on network location.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Prisma Access implements ZTNA 2.0 with least-privilege access, assessing trust continuously based on user identity, device posture, and behavior. It uses App-ID for precise application-level control, ensuring access is granted only based on strict policy enforcement, not network location.

Prompt 4: Secure Web Gateway (SWG)– Solution should include features that protect users from web-based threats, such as malware, malicious URLs, and phishing attempts, by inspecting traffic at the cloud edge and enforcing acceptable use policies.

Please describe if and how Respondent’s proposed Solution meets this above prompt in the field below.

Prisma Access SWG uses AI to detect and block web threats in real-time, offering URL filtering, malware prevention, and phishing protection. It inspects all traffic, including encrypted, at the cloud edge, ensuring secure web access and policy enforcement across all user activities.

Prompt 5: Firewall as a Service (FwaaS) – Solution should deliver consistent firewall policies across multiple locations and devices, centralizing management of security controls such as network segmentation, access control, and intrusion detection.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Prisma Access offers robust FwaaS by centralizing firewall policy management through Panorama or Strata Cloud Manager, ensuring consistent security across all endpoints. It includes advanced features like App-ID for access control, URL filtering, and threat prevention, leveraging cloud-native architecture for scalability and centralized control.

Prompt 6: Real-Time Analytics and Reporting – Solution should provide insights into network performance, traffic patterns, security threats, and user behavior across distributed environments.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Prisma Access meets the requirement for real-time analytics and reporting through several integrated features with its cloud-native architecture, ensures that these analytics are scalable, accessible from anywhere, and can adapt to the evolving landscape of cloud and distributed workforces, thereby fulfilling the requirement for comprehensive real-time analytics and reporting in a SASE framework.

Prompt 7: Integration of CTI Data Feeds – Solution should detect and block malicious network traffic or unauthorized access attempts based on real-time threat intelligence, correlating user activity and network behavior with known threat actors or compromised infrastructure.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Prisma Access can consume third party feeds in Cortex XSOAR and use the feeds to create External Dynamic List objects which are available to use in security policy constructs. We also support blocklists that can be updated programmatically from threat intel feeds via API.

Prompt 8: Cloud Access Security Broker (CASB) – Solution should integrate to provide visibility and control over cloud applications and services, monitoring and securing data stored in third-party SaaS platforms.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Prisma Access integrates CASB to offer visibility, control, and security for SaaS. It uses API-based and inline security for real-time threat prevention, data protection, and compliance, ensuring safe use of cloud apps. In addition, our AI Access Security provides visibility, control, and data protection for GenAI apps, using AI to prevent data leaks and detect threats. It integrates with existing security frameworks to manage AI application risks.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SERVICE LEVEL AGREEMENT

For Prisma Access service ("Service")

Palo Alto Networks commits to using commercially reasonable efforts to achieve certain service metrics described in sections 1.1, 1.2, and 1.3 below for Prisma Access. In the unlikely event that Palo Alto Networks does not meet these commitments, Customers will be eligible to receive a service credit. Customers must follow the Prisma Access configuration guidance in the product datasheet, deployment guides and technical documents (https://docs.paloaltonetworks.com/prisma/prisma-access).

This Service Level Agreement applies solely to Prisma Access core services, other Palo Alto Networks products and add-ons have separate service level agreements or service level objectives.

1. Service Level Commitments

1.1 Uptime Availability SLA. If, during any calendar month, the Service availability falls below 99.999%, Customer can submit a claim for credit, calculated as follows:

Monthly Uptime Availability: Service Credit Percentage

Less than 99.999% but equal or greater than 99.99% (not applicable to Prisma Access for Clean Pipe): 5%

Less than 99.99% but equal to or greater than 99.9%: 10%

Less than 99.9% but equal to or greater than 99%: 15 %

Less than 99% but equal to or greater than 98%: 25%

Less than 98%: 100%

Monthly Uptime Availability is calculated as follows:

Monthly Uptime Availability (%) = (total - downtime)/(total)

Total: Total number of minutes in a calendar month

Downtime: Time the Service was down, excluding Excluded

Excluded: Time the Service wa down due to exclusions set forth in Section 1.4 below

1.2 Security Processing Latency SLA. The latency of a transaction is measured from when the Prisma Access security engine receives the network data packets for a particular transaction to the point when the same Prisma Access security engine component attempts to transmit the same data packet. For any given minute, if 1% or more packets spend more than 10ms in latency, this is considered as exceeding the Security Processing Latency threshold, except when due to the exclusions in section 1.4 below. If, during any month, the "Monthly Security Processing Latency Percentage" (calculated as set out below) falls below 99.99%, Customer can submit a claim for credit.

Monthly Security Processing Latency Percentage is calculated as follows:

Monthly Security Processing Latency (%) = (total-exceeded)/(total)

Total: Total numbers of minutes in a month

Exceeded: Total number of minutes exceeding latency threshold, excluding Excluded.

Excluded: Time exceeding latency threshold due to exclusions set forth in Section 1.4 below.

Monthly Security Processing Latency Percentage: Service Credit Percentage

Less than 99.99% but equal or greater than 99.9%: 5%

Less than 99.9% but equal to or greater than 99%: 15%

Less than 99% but equal to or greater than 98%: 25%

Less than 98%: 100%

1.3 Third-party SaaS Application Latency SLA. The latency of a transaction is measured as round trip time elapsed between when the Prisma Access regional security engine transmits the network data packets to the third-party SaaS application and receives the same packet response by the third-party SaaS application, less any response and loading times by the third- party SaaS application. The following SaaS applications are supported: Microsoft O365, Google G Suite, Salesforce, Box and Slack. If, during any calendar month, "Monthly SaaS Application Latency Percentage" falls below 99.99%, Customer can submit a claim for credit, calculated as follows:

Montly SaaS Application Latency Percentage is the percentage of minutes during one month that the third party SaaS application latency exceeds 35 ms for Americas and EMEA or 75 ms for APAC, except when due to Excludsions set forth in section 1.4:

Monthly SaaS Application Latency (%) = (Total-Excluded)/(Total)

Total: Total number of minutes in a month

Exceeded: Number of minutes SaaS Application Latency exceeded 35 ms in Americas & EMEA or 75 ms in APAC, but excluding Excluded.

Excluded: time where latency exceeded the criteria due to exclusions set forth in section 1.4 below.

Monthly Third Party SaaS Application Latency Percentage: Service Credit Percentage

Less than 99.99% but equal or greater than 99.9%: 5%

Less than 99.9% but equal to or greater than 99%: 15%

Less than 99% but equal to or greater than 98%: 25%

Less than 98%: 100%

1.4 Exclusions. This Service Level Agreement shall not apply and the Service shall be deemed available where the loss of Service results from:

1.4.1 Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

1.4.2 Failure of Customer's Internet Service Provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet; And any reasonably unforeseeable interruption or degradation in service due to actions or inactions caused by third parties or by activities outside Palo Alto Networks control, including, but not limited to, force majeure events;

1.4.3 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the Service, if the SLA would have been met if not for such failure; Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Agreement (www.paloaltonetworks.com/legal/eula)

1.4.4 Any feature or portion of the Service marked as "Beta," "Test," "Preview," or the like, indicating that the feature has not been made generally available (aka production);

1.4.5 Scheduled maintenance and scaling events, including switchover time during high availability events;

1.4.6 Route convergence time if using BGP (Border Gateway Protocol);

1.4.7 For purposes of the Security Processing Latency SLA, packets which have been given a QOS (Quality of Service) policy by the Customer are excluded;

1.4.8 For purposes of the Third-party SaaS Application Latency SLA: Downtime at the SaaS provider or SaaS service degradation events are excluded, and latency caused by traffic redirection via a non cloud default path due to a customer's configuration are excluded.

2. Administration

2.1 Notifications. Customers may, at any time, obtain Service status here (https://status.paloaltonetworks.com), which also provides region-specific status information and an alerts feature from which Customers may subscribe to receive service notifications. Detailed information regarding service maintenance notifications are published here (https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/release-definitions).

2.2 Eligibility. To qualify to receive benefits under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to trials and evaluations of the Service provided at no cost to the Customer.

2.3 Claims Process. Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a claim. If Customer believes it is entitled to a service credit, it must: (a) open a case on the Customer Support Portal (http://support.paloaltonetworks.com) within 24 hours of an outage or an incident; and (b) submit a claim on the Claim Dashboard (https://supportcases.paloaltonetworks.com/apex/Communities_Claims) within 5 business days of the outage. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly: no later than 15 days after the root cause of the outage has been determined and the case closed. Customers may check on the claim status at any time and may sign up to receive notification when the claim status changes. Adjudicated claims shall be deemed final and may not be submitted again for re-consideration.

2.4 Service Credit Calculation.

2.4.1 Service credits are calculated by multiplying the Service Credit Percentage by the proportional monthly Service fee, and further prorated by the part of the Service affected by the outage: Service Credit = Service Credit Percentage x Monthly Service fee x Service Outage (see table in section 1) (see 2.4.2) Total Service (see 2.4.4)

Service Credit = ((Service Credit Percentage)/(see table in section 1)) x ((monthly service fee)/(see 2.4.2)) x ((service outage)/(total service see 2.4.4))

2.4.2 The monthly service fee attributable to the applicable Service excludes fees arising from collateral services Customers may have purchased such as Professional or Consulting Services, if any. The monthly service fee may be calculated by dividing one- year service fee by 12, three-year service fee by 36, etc.

2.4.3 For each month, the maximum amount of service credit that Palo Alto Networks shall be liable for is 100% of the monthly service fee paid to Palo Alto Networks.

2.4.4 Service Outage and Total Service are measured in users or bandwidth depending on the Service employed (i.e.,For Prisma Access for Users, the outage impact is measured based on the number of users affected; for Prisma Access for Networks and Prisma Access for Clean Pipe, the outage impact is measured in Mbps affected).

2.4.5 If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the service credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer. If a Customer has purchased the Service directly from Palo Alto Networks, then Palo Alto Networks shall issue the service credit towards the renewal of the Service.

2.4.6 Where an outage gives rise to liability arising from sections 1.1, 1.2, and/or 1.3 above, Customer shall not be entitled to double-dip by claiming service credits for such overlap.

2.4.7 The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any claim of non-compliance of this Service Level Agreement.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“Agreement”) GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term “Product” is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose (“Evaluations”), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

“Affiliate” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Services.

“End User Data” means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

“Enterprise Program” means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

“Hardware” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“Product” means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

“Published Specifications” mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. “Software” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“Subscription(s)” means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND

EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the “QATT”) has been deployed in defense against, response to or recovery from an “act of terrorism” as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L11 – Service Category 11: Governance, Risk, and Compliance (GRC)

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Prisma Cloud

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of Evaluator's Score for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: GRC Solutions should provide a structured approach to managing governance frameworks, assessing enterprise risks, and ensuring compliance with industry regulations. The Solution must facilitate the development of policies, automate compliance checks, and enable risk management and assessment workflows that align with business objectives.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud is a comprehensive cloud security platform from Palo Alto Networks designed to secure cloud-native applications, infrastructure, and services across multi-cloud environments (AWS, Azure, Google Cloud, and more). It provides a wide range of features for visibility, compliance, governance, and protection of cloud workloads, helping organizations ensure the security, compliance, and risk management of their cloud infrastructure.

Prisma Cloud includes the following key capabilities:

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWP)
- Identity and Access Management (IAM) Security
- Cloud Native Application Protection (CNAPP)
- Cloud Compliance and Governance
- DevSecOps and CI/CD

Prisma Cloud provides end-to-end security coverage across cloud infrastructure, applications, data, and user access, giving organizations comprehensive protection against a wide range of threats. Prisma Cloud helps organizations automate compliance checks against industry standards and regulatory frameworks, reducing the risk of non-compliance penalties and making audit preparation easier. Prisma Cloud is designed to scale with your cloud infrastructure, so it can grow with your business. Whether you're securing a few cloud resources or a global multi-cloud environment, Prisma Cloud provides consistent protection.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Centralized Policy Management – Solution should allow the creation, distribution, and tracking of governance frameworks, compliance guidelines, and operational policies. The Solution should support version control and electronic signatures for policy acceptance.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud offers a centralized policy framework that allows organizations to define security, compliance, and operational policies in one place. These policies are applicable across multiple cloud providers (AWS, Azure, Google Cloud, etc.), making it easier to enforce consistent security practices. Organizations can create custom policies based on their specific security needs, risk tolerance, and compliance requirements.

Prompt 3: Risk Assessment Tools – Solution should enable organizations to identify, assess, and prioritize risks across departments or business units based on likelihood and impact.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud continuously discovers all assets within the cloud environment, including virtual machines, containers, serverless functions, storage buckets, network configurations, databases, and third-party services. This ensures no resource goes undetected and that potential risks in hidden or overlooked assets are identified. It provides visibility into configurations and policies across major cloud platforms like AWS, Azure, Google Cloud, and others.

Prompt 4: Risk Mitigation and Treatment Workflows – Solution should allow teams to define and track risk response plans, assign responsibilities, and monitor progress toward mitigation goals.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud generates detailed risk treatment reports that document each step taken to mitigate a risk. This includes information on the identified risks, the actions taken, and the current status of the remediation. Prisma Cloud also supports the integration of approval workflows, ensuring that remediation actions are properly authorized before being applied. This helps avoid accidental changes or configurations that may introduce new risks.

Prompt 5: Audit Management Capabilities – Solution should support the planning, scheduling, and execution of internal and external audits. The platform should automatically generate audit reports, track findings, and ensure follow-up actions are completed.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud's audit management allows continuous tracking and documenting of activities within the cloud infrastructure, ensuring they meet regulatory requirements, quickly respond to security incidents, and continuously improve security practices. Prisma Cloud includes built-in compliance frameworks that automate auditing of cloud environments. Detailed and customizable audit reports ensure organizations can demonstrate compliance with minimal effort.

Prompt 6: Compliance Tracking – Solution should include industry-specific regulations (e.g., NIST CSF, GDPR, HIPAA, PCI-DSS), with automated controls and real-time monitoring to detect non-compliance or control failures.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud continuously monitors cloud environments and supports more than 20 compliance standards, including PCI DSS, HIPAA, GDPR, SOC 2, NIST 800-171, NIST 800-53, NIST CSF, ISO 27002, CCPA, CCM and any custom framework.

Prompt 7: Customizable Risk Dashboards – Solution should provide executives with an overview of key risks, compliance metrics, and the overall health of the governance program. Dashboards should display real-time data and support drill-down views for detailed analysis.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Customizable Risk Dashboards allow users to create personalized, role-based dashboards focusing on specific risk areas most relevant to their organization. The dashboards provide a unified view of security posture across cloud environments giving the ability to visualize, prioritize, and track risk indicators for their assets and workloads. In addition, they include historical data for trend analysis, which allow to track security and compliance performance over time.

Prompt 8: Third-Party Risk Management – Solution should facilitate the assessment of third-party vendor risks and perform due diligence on vendors' compliance and risk management practices.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prisma Cloud provides tools to assess, monitor, and reduce the risks posed by 3rd party relationships, ensuring cloud infrastructure and data remain secure, compliant, and resilient. Prisma Cloud helps organizations manage and mitigate the risks associated with their 3rd party vendors, services, and integrations in cloud environments. As organizations increasingly rely on 3rd party providers it becomes crucial to assess and manage the security and compliance risks.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SERVICE LEVEL AGREEMENT

Prisma Cloud Subscription Service

Palo Alto Networks will use commercially reasonable efforts to make its Prisma Cloud SaaS Subscription service ("Service") meet 99.9% Monthly Uptime Availability as set forth herein ("Service Level"). In the unlikely event that Palo Alto Networks does not meet this Service Level commitment, Customers will be eligible to claim a service credit as described below ("Service Credit").

1. Service Level Commitment

Palo Alto Networks will use commercially reasonable efforts for the Service to maintain a Monthly Uptime Availability of at least 99.9%, which is calculated as follows:

Monthly Uptime Availability Percentage = ((total time - downtime)/(total time)) x 100%

Total Time: Total number of minutes in a calendar month.

Downtime: Total number of minutes Customer lost external connectivity to the Prisma Cloud Console in a calendar month, excluding the number of minutes that meet the criteria under Section 2 - Exclusions.

2. Exclusions

Unavailability of the Service due to the following reasons shall be excluded from the Downtime, as provided for above:

2.1 Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

2.2 Failure of Customer's internet service provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;

2.3 Any reasonably unforeseeable interruption or degradation in Service due to actions or inactions caused by third parties or by activities outside Palo Alto Networks control, including, but not limited to, force majeure events;

2.4 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the Service, if the SLA would have been met if not for such failure;

2.5 Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Licensing Agreement (www.paloaltonetworks.com/legal/eula), unless Customer and Palo Alto Networks have entered into a separate written agreement that specifically overrides such End User Licensing Agreement;

2.6 Any feature or portion of the Service marked or licensed to Customer as “Beta,” “Test,” “Preview,” or the like, indicating that the feature has not been made generally available (aka production);

2.7 Scheduled and unplanned maintenance windows;

2.8 High Availability events and scaling events.

2.9 Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate Service under this Service-Level Agreement.

3. Service Credit Claim

3.1 Service Credits. In the event that a Customer reasonably believes that the Service Level in connection with Customer’s use of the Service is not met in any calendar month, Customer may file a claim for Service Credit pursuant to Section 3.2 below. Once verified by Palo Alto Networks, Downtime shall begin to accrue from the time Customer notifies Palo Alto Networks pursuant to Section 3.2 and will continue to accrue until the Service is restored. Subject to the terms and conditions herein, for a qualified Claim, Palo Alto Networks will issue a Service Credit which equals to 2% of monthly Service fees when there is a period of at least sixty (60) consecutive minutes where Monthly Uptime Availability is not met, provided that: (1) no more than one Service Credit will be issued in any calendar day; and (2) for each calendar month, the maximum amount of Service Credit that Palo Alto Networks shall be liable for is one (1) week of the monthly Service Fee received by Palo Alto Networks.

3.2 Claims Process. Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a Claim. If Customer believes it is entitled to a Service Credit, it must open a case on the Customer Support Portal (http://support.paloaltonetworks.com) within 24 hours of the start of the outage. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly and in good faith based on its technical records and the information provided by the Customer. Customers may check on the Claim status at any time and may sign up to receive notifications when the Claim status changes. Adjudicated Claims shall be deemed final and may not be submitted again for re-consideration.

3.3 Claim Eligibility. To qualify to receive benefits under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to trials or evaluations of the Service that are provided at no cost to the Customer.

4. Miscellaneous

4.1 Notifications. Customers may, at any time, obtain Service status updates at https://status.paloaltonetworks.com, which also provides region-specific status information and an alerts feature from which Customers may subscribe to receive Service notifications.

4.2 Applicability. The monthly Service fee attributable to the applicable Service excludes fees arising from additional services Customers may have purchased, such as Professional Services or consulting services, if any. The monthly Service fee may be calculated by dividing one-year Service fee by 12, three-year Service fee by 36, etc.

4.3 Distributor & Reseller Orders. If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the Service Credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer. If a Customer purchased the Service directly from Palo Alto Networks, then Palo Alto Networks shall issue the Service Credit towards the next renewal of the Service.

4.4 Entire Liability. The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any Claim of non-compliance of this Service Level Agreement.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term "Product" is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS "CUSTOMER", "END USER", "YOU" or "YOUR") AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS "PALO ALTO NETWORKS").

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

“Affiliate” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Services.

“End User Data” means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

“Enterprise Program” means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

“Hardware” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“Product” means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

“Published Specifications” mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. “Software” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“Subscription(s)” means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED “AS IS”. PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks’ suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks’ suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the

Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer’s payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party’s patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a “Claim”), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks’ requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks’ prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks’ opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks’ reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks’ obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Armix VIPR Pro

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Vulnerability Assessment and Management Solutions must enable organizations to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts. The Solution should automate both scanning and remediation workflows, providing real-time visibility into the organization's security posture.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Armis Centrix™ For VIPR - Prioritization and Remediation introduces unparalleled advancements by going beyond vulnerability management to find and consolidate security findings across all sources to holistically understand risk and automate prioritization. Armis Centrix™ streamlines the entire remediation lifecycle, from identifying owners to operationalizing fixes, providing a unified platform for prioritization and efficient risk resolution management. Armis Centrix™ revolutionizes how organizations mitigate high-risk findings, empowering them to stay ahead of evolving threats and safeguard their organization with confidence.

We consolidate all detection tool findings and deduplicate alerts, providing an aggregated view of all findings. from on-premise hosts and endpoints to code, cloud services and application security tools.

Our technology assigns context to findings, including threat intelligence, likelihood of exploit, and asset attributes like business impact and compliance policies. The result is a consolidated set of prioritized findings based on organization-specific risk concerns.

Armis generates predictive ownership rules through AI to assign fixed responsibilities and enables ongoing communication with distributed teams.

Advanced dashboards help security leaders measure the effectiveness of the remediation process and produce executive stakeholder reporting.

Key Differentiators that make Armis the go to approach:

- Streamline risk assessment & remediation.
- Adaptable prioritization for risk identification.
- Integrated asset inventory and enrichment.
- Predictive AI for remediation ownership.
- Consolidated remediation activity monitoring.
- Effective collaboration through bidirectional workflows integrations.
- Centralized visibility into risk posture.

Why more businesses are trusting Armis to drive measurable outcomes

- 50-1 backlog reduction with alert consolidation and ML deduplication.
- 90% improved MTTR for prioritized findings.
- 80% time savings by automating assessment.

• 90% Remediation task efficiency improvement through ownership assignment and ticket automation.

• 7x increase in the number of closed findings on an annualized basis.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Automated and Continuous Vulnerability Scanning – Solution should include automated and continuous scanning of network devices, servers, endpoints, and applications. The scans should identify known vulnerabilities (e.g., CVEs), misconfigurations, and missing patches.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

The Armis solution is built on an architecture that provides a continuous and passive ingestion of data from multiple data sources. This approach provides up to date vulnerability information for all assets, including virtual, IOT/OT, Servers, Clients, Applications, and other endpoints. This level of visibility and context empowers a complete understanding of all vulnerabilities with subsets that include CVEs, misconfigurations, security patches, code and web application security bugs, and more.

Prompt 3: Risk-Based Vulnerability Prioritization – Solution should allow vulnerabilities to be sorted and ranked based on the criticality of the affected asset, the exploitability of the vulnerability, and the business impact. This helps organizations focus on high-priority issues that pose the most risk.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Armis VIPR analyzes ingested data from all security findings tools which it then prioritizes based on both security findings and asset The prioritization utilizes key factors like security risk, business impact, criticality, and other contextual factors including: behaviors, threats, and real world exploitability.

Prompt 4: Remediation Workflows – Solution should integrate with IT service management (ITSM) systems, automatically creating tickets or work orders for IT teams to address vulnerabilities, track progress, and close issues once remediated.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

By offering predictive ownership assignment and bidirectional communication integrated with users' workflow and collaboration tools, Armis VIPR Pro provides flexibility to work within existing ticketing systems or via email directly. The VIPR workflow supports common tasks like exceptions and false positives while simultaneously tracking SLA, MTTR, compliance and justifications.

Prompt 5: Detailed Vulnerability Reports – Solution should include the ability to provide reports including information such as affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

VIPR reports provide grouped fixes by remediation while also providing breakdown information, including remediation owner, asset owner, security findings, threat and CVE details, remediation guidance, ticketing information, and more. Users can view the reports for the whole organization or for a segmented portion (like a type of asset, region, type of issue, team/business unit, etc.). We also provide dynamic campaign views for users to track ongoing remediation efforts.

Prompt 6: Real-Time Insights and Trend Analysis – Solution should provide insights into the overall security posture, such as the number of open vulnerabilities, time-to-remediation, and patch compliance rates.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

VIPR admins and analysts can monitor the vulnerability status of their environment, from cloud to ground. With real time capabilities to report on trends, SLA, policy compliance, ticket status, and organizational risk posture, VIPR presents a view for every team member. VIPR also tracks security tool gaps and overlaps providing explainability behind the data.

Prompt 7: Integration with Patch Management Solutions – Solution should allow organizations to deploy patches to vulnerable systems directly from the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

VIPR empowers organizations to automate the remediation by customizing your current technology capabilities. VIPR acts as the nerve center for your vulnerability management program by building a holistic view of all vulnerabilities, consolidating them into fixes, and streamlining the workflow outputs and tracking.

Prompt 8: Integration of CTI Data Feeds – Solution should enhance vulnerability prioritization by providing real-time threat intelligence on active exploitation campaigns, emerging threats, or vulnerabilities that are being specifically targeted by threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

The Armis Threat Intelligence Engine includes out of the box rules for many exploits, vulnerabilities and misconfigurations. The threat engine is externally loaded with all known malware and vulnerability signatures continuously to include for example: NIST, NVD, ICS-CERT, FDA, DHS security advisories, vendor bulletins, compliance databases, and many more. With the Armis ATI module, additional threat intelligence is added for previously undisclosed exploited vulnerabilities.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Armis will use commercially reasonable efforts to maintain Uptime Availability of at least 99.9% per month as monitored by Armis’ Platform availability monitoring systems.

Armis offers Service Level Objectives for the initial response to Customer support tickets based on the severity of the Customer impact. The ticket priority is based on the business impact as described below:

Armis offers Service Level Objectives for the initial response to Customer support tickets based on the severity of the Customer impact. The ticket priority is based on the business impact as described below:

• Critical (Severity 1) - The Platform is down, all functionalities are not operational and the issue is directly disrupting customer network and/or business operations. No reasonable workaround is available. Support will respond within 1 hour and will work continuously until the issue is fixed.

• High (Severity 2) - A major Platform functionality is impacted by an issue that is persistent and affects many users. No reasonable workaround is available. Support will respond within 8 business hours and will work through the normal business day.

• Medium (Severity 3) - Platform is operational, with a minor impact on functionality for some or all users, and an acceptable workaround or solution exists. Support will respond within 2 business days and will reasonably work through the issue as resources are available.

• Low (Severity 4) - Minor issues not impacting Platform functionality. Support will respond within 4 business days and will reasonably work through the issue as resources are available.

ARMIS PLATFORM TERMS AND CONDITIONS

These Armis Platform Terms and Conditions (these “Terms”) are between the Armis entity identified in Section 16.1 below (“Armis”) and the customer who purchased the subscription to the Armis Solutions (“Customer”). Armis and Customer may be referred to individually as a “Party” or collectively as the “Parties.” Capitalized terms used in these Terms have the meanings assigned to such terms as designated herein. Unless Customer and Armis have signed another agreement which expressly governs Customer’s subscription to and use of the Armis Solutions and overrides these Terms, by accepting these Terms via the signing or otherwise indicating acceptance of an applicable Purchase Order, by clicking through to access the Armis Platform, or by otherwise indicating Customer’s acceptance of these Terms through access to and/or use of the Armis Solutions (and such date, the Effective Date unless another date is indicated in the Purchase Order as described in Section 4.1), Customer agrees to be bound by these Terms and the person acting on Customer’s behalf hereby represents to Armis that they have the authority to bind Customer to these Terms through such consent or access to the Armis Solutions. If Customer does not agree to these Terms or you do not have the authority to bind Customer to these Terms, then Customer may not access to or use the Armis Solutions. The Parties agree as follows:

1. Definitions.

1.1 “Affiliate” means any entity that directly, or indirectly through intermediaries, controls, is controlled by, or is under common control with a Party.

1.2 “Armis APIs” means the Armis’ proprietary application programming interfaces and /or software development kits (SDK) made available to Customer for use in integrating the Armis Platform with other products and applications, in each case solely in accordanceArmis API/SDK License Agreement available here: https://www.armis.com/legal-compliance/.

1.3 “Armis Assets” means: (i) the Armis Solutions and Documentation; (ii) Armis APIs; and (iii) all specifications, technology, software (including all underlying source code and object code), data, methodologies, machine learning models, user interfaces, algorithms, enhancements, components, documentation, techniques, designs, inventions, works of authorship, and know-how, in each case, that are used to provide, or made available in connection with, any of the Armis Solutions , and in each case all associated Intellectual Property Rights, and any subsequent updates, upgrades, and derivatives of any of the foregoing.

1.4 “Armis Platform” means (i) the Armis Software as a Service (SaaS) products (“Armis SaaS”); (ii) Collectors; and (iii) Collector Technology.

1.5 “Armis Solutions” means: (i) the Armis Platform; (ii) Armis APIs; and (iii) Professional Services.

1.6 “Authorized User” means any individual who accesses or uses the Armis Solutions on behalf of Customer or its Affiliates.

1.7 “Collector” means hardware, if any, such as servers or network ports, provided by or on behalf of Armis to Customer to enable the use of the Armis Platform.

1.8 “Collector Technology” means Armis’ virtual machine images or Collector-related software provided by or on behalf of Armis to Customer to enable use of the Armis Platform.

1.9 “Customer Data” means Customer’s data automatically collected, processed, hosted by the Armis Platform through Customer’s use of the Armis Solutions, including copies, modifications, and other derivatives of such data that is generated by the Armis Platform through Customer’s use of the Armis Platform. Customer Data does not include Statistical Data.

1.10 “Documentation” means any technical user guides, manuals, release notes, installation notes, specifications, “read-me” files, support guides, and other materials related to the Armis Solutions, and the use, operation, and maintenance thereof, including all enhancements, modifications, derivative works, and amendments to the same, in each case, that Armis publishes or provides to Customer through its Support Portal available at: https://support.armis.com/s/login (or any successor website, “Support Portal”).

1.11 “Intellectual Property Rights” means all patents, copyrights, moral rights, trademarks, trade secrets, and any other form of intellectual property rights recognized in any jurisdiction, including applications and registrations for any of the foregoing.

1.12 “Laws” means, collectively, any laws, statutes, ordinances, regulations and other types of government authority, promulgated under such authority anywhere in the world.

1.13 “Partner” means an authorized Armis partner, including a reseller, marketplace, or implementation partner.

1.14 “Purchase Order” means: (i) an order form executed by Armis and Customer; or (ii) a purchase order, statement of work, or other similar document issued by Customer or a Partner in each case solely to the extent its terms match and do not deviate from a corresponding Quote. In the event of a conflict between a Purchase Order and a Quote, the Quote will control. If Customer orders Armis Solutions through a Partner or marketplace, then such Partner’s or marketplace’s applicable ordering document will apply solely with respect to the fees payable by Customer, volumes, and subscription term of Armis Solutions ordered.

1.15 “Quote” means a quote prepared and issued by Armis to Customer or a Partner that forms part of these Terms and describes the Armis Solutions ordered by Customer and any associated terms and fees.

1.16 “Professional Services” means any services (beyond the Armis support provided pursuant to Section 2.3.1) such as advisory, consulting, implementation, integration, or training services, that may be provided by or on behalf of Armis to Customer as detailed in an applicable Purchase Order.

1.17 “Statistical Data” means data generated in relation to Customer’s use of the Armis Platform that has been irreversibly anonymized as to Customer and aggregated by Armis. Statistical Data includes generic device descriptions and performance metadata about devices that appear in Customer’s instance of the Armis Platform, such as the device manufacturer, type of operating system, and device model. Statistical Data does not include: (i) any identifiers that would link any devices to Customer, such as IP addresses, MAC addresses, or unique Customer identifiers; or (ii) any data processed on or hosted by any Customer device.

2. Armis Platform.

2.1 Access and Use. During the Subscription Term and subject to Customer’s compliance with these Terms, Armis grants Customer a subscription to access and use the Armis Platform. Customer shall only use the Armis Platform in accordance with the Documentation, solely for Customer’s internal business purposes, and subject to any use limitations indicated in the applicable Purchase Order. The rights granted to Customer herein includes the right to deploy and use the Armis Platform at Customer’s Affiliates’ environments, provided Customer remains fully responsible and liable under these Terms for Customer’s Affiliates’ use. In addition to any access rights a Customer Affiliate may have as aforesaid, a Customer Affiliate may separately subscribe to Armis Solutions pursuant to these Terms by entering into a Purchase Order, and in each case, all references in these Terms to Customer will be deemed to refer to the applicable Affiliate for purposes of that Purchase Order.

2.2 Customer Responsibilities. The Armis Platform may be used by or for Customer only through an account that is specific to Customer and only by Authorized Users. Customer is solely responsible for: (i) identifying and authenticating all Authorized Users, approving access by such Authorized Users to the Armis Platform, and ensuring each Authorized User complies with these Terms; (ii) ensuring that Authorized Users keep their login credentials safe and secure; (iii) all activities that occur under the login credentials of Authorized Users; and (iv) the accuracy, quality, and legality of Customer Data, the means by which Customer acquired Customer Data, Customer's use of Customer Data with the Armis Platform, and the interoperation of any Non-Armis Products with which Customer uses the Armis Platform. Armis is not responsible for any losses or damages arising due to any breach of these Terms by any Authorized User or any other personnel, agent, or advisor of Customer. Customer shall notify Armis immediately upon becoming aware of any unauthorized access to or use of the Armis Platform.

2.3 Provision of the Armis Solutions.

2.3.1 Support. Armis shall provide Customer with standard support (at no additional cost) unless Customer purchases upgraded support as set forth in a Purchase Order. Armis shall provide the technical support and service level commitments set forth in Armis' Platform Support Terms ("SLA"), as updated from time to time, available in the Support Portal. Except for critical updates, Armis schedules maintenance during non-peak usage hours (that reasonably minimizes the impact on all customers worldwide) and shall provide reasonable advance notice through the Armis Platform of any planned downtime in accordance with the SLA.

2.3.2 Updates. Armis makes updates (e.g., bug fixes, enhancements) to the Armis Platform on an ongoing basis, which are delivered through the Armis Platform. Customer's subscription includes all updates that Armis makes generally available to its customers at no additional charge. To the extent Customer's configuration of the Armis Platform requires acceptance of updates, Customer shall accept such updates in a timely manner. Armis is not responsible for the proper performance of the Armis Platform or for any security issues encountered with the Armis Platform resulting from any delay or failure to accept such updates. Armis may update the content, functionality, and user interface of the Armis Platform from time to time, provided that such update will not materially decrease the functionality of the Armis Platform during the Subscription Term. Customer's use of the Armis Solutions under these Terms is not contingent on the delivery of any future features or functionality.

2.3.3 Subcontractors. Armis may utilize subcontractors in the provision of the Armis Solutions, including to process

Customer Data, provided that such subcontractors: (i) are subject to confidentiality obligations materially as protective of Customer Data as those set forth herein; and (ii) maintain commercially reasonable technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Data, taking into account the state of the art, costs of implementation, and the type of data. Armis will be liable for the acts and omissions of its subcontractors to the extent such acts or omissions constitute a breach of these Terms.

2.4 Professional Services. During the Subscription Term, Customer may receive Professional Services subject to these Terms as detailed in a Purchase Order. If applicable, the Armis Quote for Professional Services will identify any additional terms that apply with respect to such Professional Services.

2.5 Data Protection and Security. Armis shall implement and maintain commercially reasonable technical, physical, and organizational measures designed to protect the security, confidentiality, and integrity of Customer Data, taking into account the state of the art, costs of implementation, and the type of data, in accordance with Armis' information security program, as updated from time to time. Any updates to Armis' information security program will not materially diminish Armis' current data security obligations, a summary of which is available at: https://www.armis.com/legal-compliance/information-security-disclosure/ (or successor website). In addition, the terms and conditions of Armis' Data Processing Addendum ("DPA") found at https://www.armis.com/legal-compliance/data-processing-addendum/ (or successor website), apply to the processing of any Personal Data (as defined in the DPA). Armis shall promptly notify Customer upon becoming aware of a breach the aforementioned security measures within Armis' network leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data ("Security Incident"), and Armis shall reasonably cooperate with Customer in the investigation and mitigation thereof. Armis' obligation to report or respond to a Security Incident is not an acknowledgement by Armis of any fault or liability with respect to such Security Incident. In addition, Armis shall use commercially reasonable efforts to respond, once per year, to any reasonable written inquiries from Customer regarding compliance with this Section 2.5, including requests for Armis' most recent third-party auditor reports regarding Armis' information security program.

2.6 Non-Armis Service Providers. Customer may engage one or more third parties to manage the installation, onboarding, and/or operation of the Armis Platform on Customer's behalf ("Non-Armis Service Provider"), provided that Customer delivers written notice to Armis in advance of such engagement. Customer shall require the Non-Armis Service Provider to comply with these Terms and shall ensure that such Non-Armis Service Provider uses the Armis Platform solely on behalf of Customer. Customer will be fully liable for the acts and omissions of its Non-Armis Service Providers to the extent such acts or omissions constitute a breach of these Terms.

2.7 Non-Armis Products. Customer may from time to time decide to use an integration between Non-Armis Products and the Armis Platform. "Non-Armis Products" means third-party products, applications, services, software, networks, or other systems or information sources acquired by Customer that are not developed by Armis or provided by Armis as part of the Armis Platform. Use of Non-Armis Products is subject to the end user license or other agreement between Customer and the provider of the Non-Armis Products. Armis has no liability with respect to the implementation, maintenance, use, or continued interoperability of any Non-Armis Products, even if Armis designates them as approved or recommended or is an authorized reseller of such Non-Armis Products. By enabling any interoperability between Non-Armis Products and the Armis Platform, Customer expressly agrees to the transfer of any Customer Data between Armis and the provider of the Non-Armis Product as required for such interoperability.

2.8 Restrictions. Customer and its Authorized Users shall not, and shall not authorize any third party to: (i) decompile, disassemble, reverse engineer, copy, frame, or mirror any part of the Armis Assets, or otherwise attempt to derive the source code, structure, ideas, algorithms, or associated know-how of any Armis Assets; (ii) translate, adapt, or modify any Armis Assets; (iii) write or develop any program based upon any Armis Assets, or otherwise access, test, or use any Armis Assets for the purpose of developing or distributing products or services that compete with any Armis Assets; (iv) sell, sublicense, transfer, assign, lease, rent, distribute, grant a security interest in, or otherwise commercially exploit any Armis Assets or make available to a third party any Armis Assets except as expressly authorized in these Terms; (v) use the Armis Assets other than as expressly permitted by these Terms and solely for Customer's internal business operations and in conformity with the Documentation; (vi) alter or remove any trademarks or proprietary notices contained in or on the Armis Assets;

(vii)attempt to gain access to the Armis Platform or its related systems or networks through unauthorized means, including any automated means (i.e., use of scripts or web crawlers), circumvent or interfere with any authentication or security measures of the Armis Platform, or otherwise interfere with or disrupt the integrity or performance of the Armis Platform;

(viii) probe, scan, or test the vulnerability of any Armis system or network; (ix) conduct any competitive analysis, publish or share with any third party any results of any technical evaluation or benchmark tests performed on Armis Assets, or disclose Armis Assets' features, errors, or bugs to a third party without Armis' prior written consent; or (x) use any portion of the Armis Assets in violation of any applicable Laws or transmit to or from the Armis Assets any data, materials, or other content that infringes, misappropriates, or otherwise violates any third-party rights. Customer shall promptly notify Armis in writing if it becomes aware of, or has reason to believe, that any of the prohibitions in this Section have been

breached by Customer, its Affiliates or any Authorized User.

3. Collectors. The Armis Platform may include Collectors that are provided to Customer during the Subscription Term under an applicable Purchase Order. Customer shall use and reasonably maintain Collectors in good working order in accordance with the Documentation and at the locations agreed to by the Parties to enable proper usage and operation of the Armis Platform. Support for Collectors is provided pursuant to Armis' standard support services, as described in the SLA and in the Documentation, which may require installation of a current release of Collector Technology. Without Armis' express written permission, Customer shall not, and shall not permit any third party to: (i) use Collectors other than for the express purpose for which they were provided; (ii) rent or lease Collectors to any third party; (iii) transfer or copy the Collector Technology within the Collector to any other product or device; or (iv) install the Collector Technology on any device other than the applicable Collector for which it was provided. The Armis Platform may not operate as intended if Collectors are moved to any other geographic location without Armis' prior express written permission.

4. Purchase Orders and Fees.

4.1 Subscription Term and Purchase Orders. Each Purchase Order will commence on the subscription start date (the "Effective Date") stated in such Purchase Order and continue until the subscription end date stated therein ("Subscription Term"). Unless otherwise specified in a Purchase Order: (i) subscriptions for the Armis Solutions will automatically renew for additional one (1) year terms unless either Party gives the other written notice (email acceptable) at least thirty (30) days before the end of the relevant Subscription Term; (ii) discounts or other promotional pricing offered for the Armis Solutions are one-time and valid only for the specific amount purchased; (iii) renewal of any discounted Armis Solutions will be at Armis' applicable list price then in effect, and any change in the amount of, or term for, the Armis Solutions may result in re-pricing without regard to prior pricing; and (iv) during a Subscription Term, any purchase of additional amounts will be priced at Armis' applicable list price then in effect.

4.2 Fees. For direct purchases from Armis, Customer shall pay Armis the fees and other amounts detailed in any applicable Purchase Order in accordance with the terms therein. If applicable, Customer shall reimburse Armis for reasonable, documented, out-of-pocket expenses (including all travel costs and expenses) that are authorized by Customer in writing and that are incurred by

Armis in the course of providing Professional Services. If Customer's use of the Armis Solutions exceeds the usage limitations set forth in the applicable Purchase Order, then Armis may invoice Customer, and Customer shall pay, for such excess usage at Armis' then current rates, prorated for the remainder of the Subscription Term. Upon renewal, Customer's subscription will be increased to reflect Customer's actual usage during the preceding Subscription Term. Armis Solutions purchased cannot be decreased during a Subscription Term.

4.3 Payment Terms. Armis' obligations under these Terms are conditioned on Customer's payment in full of the fees when due as set forth in the applicable Purchase Order. For direct purchases from Armis, all fees are billed annually in U.S. Dollars with net thirty (30) payment terms, unless alternate terms are stated in the applicable Purchase Order. Customer shall make any good faith dispute of an invoice in writing within thirty (30) days of the applicable invoice date. If Customer (or a Partner through whom Customer purchased) fails to pay any amounts set forth in a Purchase Order when due, Armis reserves the right to suspend Customer's access to the Armis Solutions thirty (30) days following Armis' written notice to Customer of nonpayment until Armis receives payment in full. Any fees not paid when due or not subject to a good faith dispute will accrue interest on a daily basis until paid in full at the lesser of: (i) the rate of one percent (1%) per month; and

(ii) the highest amount permitted by applicable law. Except as expressly stated in these Terms, all fees due or paid are non- cancellable and non-refundable. Neither Party may set-off fees payable under these Terms or a Purchase Order against any other amounts owed to such Party. Customer requirements for purchase orders, vendor registration forms, vendor portals, or the like, will not change Customer's payment obligations herein.

4.4 Taxes. All amounts payable under these Terms are exclusive of all sales, use, value-added, withholding, and other direct or indirect taxes, charges, levies, and duties, and all such amounts are Customer's sole responsibility, provided that Customer is not responsible for any taxes on Armis income. These taxes (if applicable) will be stated separately on each invoice, unless Customer provides (in advance) a valid tax exemption certificate authorized by the applicable taxing authority. In addition, if applicable law requires Customer to withhold any amounts on payments owed to Armis pursuant to these Terms, Customer shall: (i) effect such withholding and remit such amounts to the appropriate taxing authorities; and (ii) ensure that, after such deduction or withholding, Armis receives and retains, free from liability for such deduction or withholding, a net amount equal to the amount Armis would have received and retained in the absence of such required deduction or withholding.

5. Beta Products. FROM TIME TO TIME, ARMIS MAY OFFER CUSTOMER THE OPPORTUNITY (WHICH CUSTOMER MAY REFUSE IN ITS SOLE DISCRETION) TO USE EARLY AVAILABILITY OR BETA PRODUCTS, FEATURES, OR DOCUMENTATION (COLLECTIVELY, "BETA PRODUCTS"). BETA PRODUCTS MAY NOT BE GENERALLY AVAILABLE, ARE PROVIDED STRICTLY "AS IS," AND WILL NOT BE SUBJECT TO ANY REPRESENTATIONS, WARRANTIES, INDEMNIFICATION OBLIGATIONS, OR SUPPORT OBLIGATIONS. UNLESS

PROHIBITED BY LAW, ARMIS WILL HAVE NO LIABILITY RELATED TO SUCH BETA PRODUCTS IN EXCESS OF ONE THOUSAND USD ($1,000.00 USD). CUSTOMER OR ARMIS

MAY TERMINATE CUSTOMER'S ACCESS TO BETA PRODUCTS AT ANY TIME FOR ANY OR NO REASON.

6. Ownership and Reservation of Rights.

6.1 Armis. Except for the rights expressly granted to Customer in Section 2.1, as between the Parties, Armis and/or its licensors own and retain all rights, title, and interest, including Intellectual Property Rights, in and to all Armis Assets, Armis Confidential Information, and any other tangible and intangible material and information incorporated into or constituting any portion of the Armis Assets (excluding any Customer Data and Customer Confidential Information).

6.2 Customer. Except for the rights expressly granted to Armis in this Section 6, as between the Parties, Customer owns and retains all rights, title, and interest in and to Customer Data, Customer Confidential Information, and Feedback, including all associated Intellectual Property Rights. During the Subscription Term, Customer shall provide to Armis the right to access, process, transmit, store, use, and disclose Customer Data as necessary to provide the Armis Solutions to Customer and to improve the Armis Solutions including to identify, investigate, or resolve technical problems with the Armis Solutions.

6.3 Feedback. Customer or an Authorized User may provide to Armis, directly or indirectly, feedback, analysis, suggestions, or comments about the Armis Assets or Armis Solutions (collectively, "Feedback"). Feedback does not include Customer Data or Customer Confidential Information. Customer hereby grants to Armis a non-exclusive, perpetual, irrevocable, transferable, royalty-free, and worldwide right, with the right to grant and authorize sublicenses, to use and benefit from such Feedback to provide and improve the Armis Assets and Armis' business without any compensation or credit due to Customer.

6.4 Statistical Data. During the Subscription Term, Armis may collect and compile Statistical Data and Armis owns and retains all rights, title, and interest in such Statistical Data. Armis may use Statistical Data for its own business purposes (such as improving, testing, and maintaining the Armis Solutions, including training Armis' machine learning algorithms and artificial intelligence models associated with the Armis Solutions, identifying trends, and developing additional products and services).

6.5 Reservation of Rights. Each Party retains all rights that are not expressly licensed to the other Party in these Terms and does not grant the other Party any implied licenses in these Terms or under any other theory.

7. Confidentiality.

7.1 "Confidential Information" means any non-public information disclosed in any form or manner by one Party ("Discloser") to the other Party ("Recipient") that is marked as "confidential" or that Recipient knows or reasonably should know is confidential information of Discloser given the nature of such information and the circumstances of its disclosure. Confidential Information of Armis includes the Documentation, auditor reports, security test results and reports, and all communications related to updates to the Armis Assets. Confidential Information does not include Customer Data automatically uploaded to, processed and hosted by the Armis Platform (the security and protection of which is governed by section 2.5), or any information which Recipient can demonstrate through reasonable evidence: (i) is or becomes generally known and available to the public through no act of Recipient; (ii) was already in Recipient's possession without a duty of confidentiality owed to Discloser at the time of receipt; (iii) is lawfully obtained by Recipient from a third party who has the express right to make such disclosure; or (iv) is independently developed by Recipient without breach of an obligation owed to Discloser.

7.2 During the Subscription Term, Recipient may use Discloser's Confidential Information solely for the purpose of performing its obligations under these Terms. Recipient shall use the same degree of care in protecting Discloser's Confidential Information as Recipient uses to protect its own Confidential Information from unauthorized use or disclosure, but in no event less than reasonable care. Recipient shall not disclose Discloser's Confidential Information to any third party except to its employees, consultants, affiliates, agents, and subcontractors having a need to know such Confidential Information to perform their respective obligations under these Terms and who are bound by a written undertaking of confidentiality that is at least as protective of Discloser's Confidential Information as set forth herein. In addition, Recipient may disclose Discloser's Confidential Information to the extent such disclosure is required by law or order of a court or similar judicial or administrative body, provided that Recipient notifies Discloser in advance (unless legally prohibited from doing so) to enable Discloser to seek a protective order or otherwise seek to prevent or restrict such disclosure. All right, title, and interest in and to Confidential Information is and will remain the sole and exclusive property of Discloser. Recipient is solely responsible and liable to Discloser for any act, omission, or other failure to comply with the terms of the Agreement by any of its Representatives.

7.3 The use and disclosure restrictions in this Section 7 (Confidentiality) will survive the expiration or termination of these Terms for a period of three (3) years, provided that Confidential Information defined as a trade secret under any applicable

Laws shall be maintained by Recipient in confidence so long as it retains trade secret status under such Laws.

8. Warranties.

8.1 Armis Warranties.

8.1.1 Armis Platform Warranties. Armis warrants that: (i) during the Subscription Term, the current versions of the Armis Platform will perform and function materially in accordance with the Documentation under normal and authorized use in compliance with these Terms; and (ii) Armis shall maintain appropriate technical measures and periodically update the Armis Platform to prevent the introduction of software viruses, disabling devices, trojans, worms, or other software or hardware devices designed to intentionally disrupt, disable, or harm Customer's network or systems or the operation of the Armis Platform. If Customer believes the Armis Platform does not conform to the warranties in this Section 8.1.1, Customer shall promptly notify Armis in writing (in no event later than thirty (30) days from the date of discovery of the nonconformity) by submitting a support ticket via the Support Portal in accordance with the SLA. In the event of a breach of the warranties in this Section 8.1.1, Armis' exclusive responsibility, and Customer's exclusive remedy (other than any termination rights Customer may have under Section 14), will be for Armis to either correct or replace, at no additional charge to Customer, the applicable deficiency in the Armis Platform in accordance with the SLA.

8.1.2 Professional Services Warranty. Armis warrants that, during the Subscription Term, the Professional Services will be performed in a workmanlike manner in accordance with current industry standards. If Customer believes the Professional Services do not conform to the warranty in this Section 8.1.2, Customer shall promptly notify Armis in writing (in no event later than thirty (30) days from the date the Professional Services were performed) by submitting a support ticket via the Support Portal in accordance with the SLA. Armis' exclusive responsibility, and Customer's exclusive remedy, will be for Armis, at its option and expense to: (i) re-perform the applicable Professional Services that fail to meet this warranty; or (ii) issue a refund of the fees paid for the applicable non-conforming Professional Services.

8.1.3 Exceptions. The warranties set forth in this Section 8.1 will not apply to the extent the nonconformity results from or is otherwise attributable to any failure or damage caused by the actions or inactions of Customer, Authorized Users, or any person acting at Customer's direction.

8.2 Customer Warranty. Customer warrants it will have all rights necessary, including any required consents, to provide or make available to Armis the Customer Data (including personal data) or other materials in connection with its use of the Armis Solutions and to permit Armis to use Customer Data pursuant to these Terms.

9. Mutual Representations. Each Party represents that: (i) it is duly organized, validly existing and in good standing under the Laws of its jurisdiction of incorporation or organization; (ii) it has the full corporate power and authority to execute, deliver, and perform its obligations under these Terms; (iii) the person signing or clicking through these Terms on its behalf has been duly authorized and empowered to enter into these Terms; and (iv) these Terms are valid, binding, and enforceable against it in accordance with its terms.

10. Compliance with Laws. In connection with the performance of these Terms, each Party shall comply with all Laws applicable to such Party in the conduct of its business generally. In addition, if Customer's use of the Armis Solutions requires Customer to comply with industry specific Laws applicable to such use, Customer is responsible for such compliance. Customer shall not use, export, re-export, ship, or transfer the Armis Platform to any country subject to an embargo or comprehensive sanction by the U.S., EU, UN Security Council, or other applicable jurisdiction ("Embargoed Country"), or to a person or entity subje

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Palo Alto Networks Cortex XSIAM

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Vulnerability Assessment and Management Solutions must enable organizations to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts. The Solution should automate both scanning and remediation workflows, providing real-time visibility into the organization's security posture.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM offers a centralized platform for continuous vulnerability assessment, risk-based prioritization, automated remediation, and real-time visibility..

1. Continuous Vulnerability Scanning:

● XSIAM integrates with an array of vulnerability scanners, aggregating data from various sources to provide a holistic view of the attack surface.

● XSIAM maintains real-time inventory of all assets within the environment: cloud, containers, and on-premise devices. This inventory ensures cont. visibility into potential vulnerabilities as new assets are added or modified.

2. Risk-based Prioritization of Remediation Efforts:

● Threat Intelligence Correlation: XSIAM correlates vulnerability data with up-to-date threat intelligence feeds; ability to prioritize remediation efforts based on risk posed by vulnerabilities in your specific environment.

● Business Context Integration: XSIAM allows you to assign criticality levels and business function tags to assets. This business context is factored into the risk scoring process, ensuring that vulnerabilities impacting mission-critical systems or sensitive data are given top priority.

● XSIAM considers both the CVSS score (severity) and the exploitability of a vulnerability. A high-severity vulnerability with a publicly available exploit kit will naturally require more immediate attention than a low-severity vulnerability with no known exploit.

3. Automating Remediation:

SOAR Playbooks for Orchestrated Remediation: XSIAM leverages XSOAR:

● Isolating compromised or vulnerable assets.

● Patching systems with the latest security updates.

● Triggering change requests within an ITSM system.

● Running targeted vulnerability scans after remediation to confirm effectiveness.

XSIAM integrates with popular ITSM solutions, streamlining the ticketing and CM processes associated with vulnerability remediation. This integration ensures that all remediation actions are tracked, documented, and compliant with internal policies.

4. Real-Time Visibility and Actionable Insights:

XSIAM provides real-time dashboards that visualize key vulnerability management metrics. Dashboards can display:

● No. of open vulnerabilities over time.

● MTTR for different vulnerability types.

● Patch compliance rates across your asset inventory.

● Trends in vulnerability discovery and remediation.

● Customizable Reports: XSIAM allows you to generate detailed reports which can be tailored to meet specific compliance requirements or to track the progress of remediation efforts over time.

Attack Surface Compliance Violation Dashboard is a dedicated to monitoring and managing attack surface compliance violations:

● Consolidated view of all assets and compliance status against predefined security policies.

● Immediate notifications of new vulnerabilities or config. weaknesses that introduce compliance violations.

● Guidance on prioritizing remediation efforts based on severity of the violation and affected assets.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Automated and Continuous Vulnerability Scanning – Solution should include automated and continuous scanning of network devices, servers, endpoints, and applications. The scans should identify known vulnerabilities (e.g., CVEs), misconfigurations, and missing patches.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM provides an automated and continuous vulnerability scanning solution. XSIAM continuously collects telemetry, alerts, and events from all connected systems, including network devices, servers, endpoints, and applications. It then uses machine learning and AI-driven analytics to identify known vulnerabilities (such as CVEs), misconfigurations, and missing patches.

Prompt 3: Risk-Based Vulnerability Prioritization – Solution should allow vulnerabilities to be sorted and ranked based on the criticality of the affected asset, the exploitability of the vulnerability, and the business impact. This helps organizations focus on high-priority issues that pose the most risk.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM addresses risk-based vulnerability prioritization by with advanced analytics to assess and rank vulnerabilities based on the criticality of affected assets, exploitability of vulnerabilities, and potential business impact. Integrating data from the Common Vulnerability Scoring System (CVSS), threat intelligence, and the specific context of the organization's environment, XSIAM assigns a risk score to each vulnerability.

Prompt 4: Remediation Workflows – Solution should integrate with IT service management (ITSM) systems, automatically creating tickets or work orders for IT teams to address vulnerabilities, track progress, and close issues once remediated.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSIAM streamlines remediation workflows by integrating with ITSM systems, e.g. ServiceNow, to automate creation and management of tickets/work orders for addressing vulnerabilities. It automatically generates tickets when vulnerabilities are detected, assign them to appropriate IT teams, and track progress of remediation efforts. Our SOAR capabilities ensure that vulnerabilities are systematically addressed and issues are closed once remediated.

Prompt 5: Detailed Vulnerability Reports – Solution should include the ability to provide reports including information such as affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM provides detailed vulnerability reports that are customizable and can be tailored to meet specific organizational needs. This detailed reporting feature enables organizations to have a clear view of their security posture, prioritize remediation efforts, and communicate findings to stakeholders in a structured manner. The reporting capability in XSIAM allows exporting of data, analysis, notes, dashboards, tables, & charts into either PDF or DOCX or CSV.

Prompt 6: Real-Time Insights and Trend Analysis – Solution should provide insights into the overall security posture, such as the number of open vulnerabilities, time-to-remediation, and patch compliance rates.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM delivers real-time security posture insights via dynamic dashboards and reports. Visualize key metrics like open vulnerabilities, time-to-remediation, identify vulnerability trends, and make informed decisions to strengthen your security strategy. Leverage the built-in Attack Surface Compliance Violation Dashboard for enhanced visibility.

Prompt 7: Integration with Patch Management Solutions – Solution should allow organizations to deploy patches to vulnerable systems directly from the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM facilitates integration with patch management solutions, enabling organizations to deploy patches to vulnerable systems directly from the platform. XSIAM offers integrations with leading patch management solutions such as Microsoft Intune, allowing security teams to automate and streamline the patch deployment process. XSIAM can trigger automated workflows to initiate patch deployment through these integrated solutions.

Prompt 8: Integration of CTI Data Feeds – Solution should enhance vulnerability prioritization by providing real-time threat intelligence on active exploitation campaigns, emerging threats, or vulnerabilities that are being specifically targeted by threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Cortex XSIAM ingests and processes real-time threat intelligence from various sources, providing insights into active exploitation campaigns, emerging threats, and vulnerabilities specifically targeted by threat actors. This integration allows XSIAM to apply CTI data to all ingested data, enabling the platform to dynamically adjust the prioritization of vulnerabilities based on the latest threat landscape.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Service-Level Agreement

All capitalized terms not defined herein shall have the same meaning as set forth in the Palo Alto Networks End User Agreement.

Cortex XSIAM, XDR, XSOAR, and Xpanse-hosted services shall be available 99.9% of the time, measured monthly, excluding scheduled maintenance. Further, any downtime resulting from outages of third-party connections or utilities or other reasons beyond the control of Palo Alto Networks will be excluded.

Customer's sole and exclusive remedy and the entire liability of Palo Alto Networks, in connection with Cortex product service availability, shall be to credit customer 2% of monthly service fees (downtime credit) for each breach. A breach is defined as a period of 60 consecutive minutes of downtime (delays in data log ingestion are not considered downtime). Downtime shall begin to accrue as soon as customer notifies Palo Alto Networks that the service is down and will continue to accrue until service is restored.

In order to receive downtime credit, customers must notify Palo Alto Networks within 24 hours of service unavailability by initiating a help desk ticket. Failure to provide such notice forfeits the right to receive downtime credit. Such credits may not be redeemed for cash and shall not exceed one (1) week of service fees in any one (1) calendar month. Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate service under this Service-Level Agreement.

Palo Alto Networks will provide technical support based on the Customer Success Plan purchased:

- Under the Standard Plan, technical support is available via the Customer Support Portal.
- Under the Premium Plan, technical support is also available as above and by phone 24 hours per day, 7 days per week.

Customers may initiate a help desk ticket via support.paloaltonetworks.com. Palo Alto Networks will use commercially reasonable efforts to respond as follows:

Severity Level 1: Service is down; critically affects customer production environment. No workaround available yet. Standard: less than/equal to 2 hours; Premium: less than/equal to 1 hour

Severity Level 2: Service is impaired; customer production up, but impacted. No workaround available yet. Standard: less than/equal to 4 hours; Premium: less than/equal to 2 hours

Severity Level 3: A service function has failed; customer production not affected Support is aware of the issue and a workaround is available. Standard: less than/equal to 12 hours; Premium: less than/equal to 4 hours

Severity Level 4: Non-critical issue. Does not impact customer business. Feature, information, documentation, how-to, and enhancement requests from customer. Standard: less than/equal to 48 hours; Premium: less than/equal to 8 business hours

More Information

To learn more about Palo Alto Networks Support offerings, visit paloaltonetworks.com/support or contact your local account manager. For product information, visit paloaltonetworks.com/products.

Why Palo Alto Networks?

Palo Alto Networks is committed to your success in preventing successful cyberattacks. Our award-winning services and support organization give you timely access to technical experts and on- line resources to ensure your business is protected. We take our responsibility for your success seriously and continuously strive to deliver an exceptional customer experience. Our entire services organization and Authorized Support Centers are there to ensure maximum uptime and streamlined operations.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“Agreement”) GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term “Product” is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

"Affiliate" means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where "Control" means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks' use of all Palo Alto Networks Affiliates to deliver Products and Services.

"End User Data" means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

"Enterprise Program" means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

"Hardware" means hardware-based products listed on Palo Alto Networks' then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

"Product" means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

"Published Specifications" mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. "Software" means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

"Subscription(s)" means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according

to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer’s access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks’ Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks’ Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks’ and its suppliers’ sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Blackwood Associates, Inc. ('Blackwood')

Solution Name: Tenable Vulnerability Management

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 8. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 8 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 8 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-8 / 7)
  = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Vulnerability Assessment and Management Solutions must enable organizations to continuously scan their IT assets for security vulnerabilities, evaluate the risks associated with these vulnerabilities, and prioritize remediation efforts. The Solution should automate both scanning and remediation workflows, providing real-time visibility into the organization's security posture.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Tenable Vulnerability Management is a comprehensive solution designed to enable organizations to continuously scan their IT assets for vulnerabilities, assess associated risk & prioritize remediation workflows. This approach facilitates proactive risk management.

Tenable Vulnerability Management streamlines the remediation process by providing actionable insights & automated workflows. It enables security teams to efficiently address vulnerabilities by integrating with existing IT service management (ITSM) systems, facilitating seamless ticketing & tracking of remediation activities.

The platform offers comprehensive dashboards & reporting capabilities that provide real-time insights into the organization's security posture. Security teams can monitor remediation trends, benchmark progress internally & against industry peers, & make informed decisions to optimize their vulnerability management program. ￼

Tenable Vulnerability Management is designed to scale with the organization's needs, supporting a wide range of IT assets, including on-premises, cloud, & remote environments. Its flexible architecture allows for seamless integration with various security tools & technologies, ensuring comprehensive coverage across the entire attack surface.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Automated and Continuous Vulnerability Scanning – Solution should include automated and continuous scanning of network devices, servers, endpoints, and applications. The scans should identify known vulnerabilities (e.g., CVEs), misconfigurations, and missing patches.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable provides automated & continuous scanning of network devices, servers, endpoints, & applications. It identifies known vulnerabilities (CVEs), misconfigurations, & missing patches using the industry-leading Nessus scanner. The solution ensures up-to-date assessments by integrating real-time threat intelligence & provides actionable insights to address risks efficiently, empowering organizations to maintain a secure & compliant IT environment.

Prompt 3: Risk-Based Vulnerability Prioritization – Solution should allow vulnerabilities to be sorted and ranked based on the criticality of the affected asset, the exploitability of the vulnerability, and the business impact. This helps organizations focus on high-priority issues that pose the most risk.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable pioneered the Risk-Based Vulnerability Management to prioritize remediation based on risk, using the Vulnerability Priority Rating (VPR) to focus on real threats. Unlike static CVSS scores, VPR provides dynamic, risk-centric insights. Our predictive VPR score analyzes over 150 data points from threat intelligence to highlight vulnerabilities most likely to be exploited within the next 28 days, helping organizationsaddress urgent risks first.

Prompt 4: Remediation Workflows – Solution should integrate with IT service management (ITSM) systems, automatically creating tickets or work orders for IT teams to address vulnerabilities, track progress, and close issues once remediated.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable solutions offer well-documented REST APIs & an easy-to-use software development kit (SDK) as well as well documented integration with IT Service Management (ITSM) systems out-of-box like ServiceNow, Atlassina and Cherwell. https://www.tenable.com/partners/technology

Prompt 5: Detailed Vulnerability Reports – Solution should include the ability to provide reports including information such as affected assets, severity ratings (e.g., CVSS scores), vulnerability descriptions, and recommended fixes.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Tenable uses a static Severity (CVSS) & a dynamic Vulnerability Priority Rating (VPR) to quantify how urgently you should remediate a vulnerability based on its immediate risk. For each vulnerability found we provide detail description of the issue, solution for how to remediate, output from the host as validation of the issue, plugin information, risk rating details, & reference material to better understand the vulnerability. All vulnerabilities include CVEs.

Prompt 6: Real-Time Insights and Trend Analysis – Solution should provide insights into the overall security posture, such as the number of open vulnerabilities, time-to-remediation, and patch compliance rates.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Tenable has the ability to report, track & trend remediation efforts. Tenable also provides the ability for approved users to run remediation scans to verify vulnerabilities have been addressed correctly. Remediation views are automatically prioritized & the report provides detailed information on the top discovered vulnerabilities & lists the affected hosts, & steps to mitigate the risk - including CVE, BID, & vendor knowledge base article links.

Prompt 7: Integration with Patch Management Solutions – Solution should allow organizations to deploy patches to vulnerable systems directly from the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

In addition to providing an API for users, Tenable has pre-built integrations with patch management systems for patch auditing & delta reporting against scan findings include Microsoft WSUS/SCCM, Redhat Satellite, IBM Tivoli Endpoint Manager, Altiris, VMWare Go. For a full list of integration partners, please visit: https://www.tenable.com/partners/technology.

Prompt 8: Integration of CTI Data Feeds – Solution should enhance vulnerability prioritization by providing real-time threat intelligence on active exploitation campaigns, emerging threats, or vulnerabilities that are being specifically targeted by threat actors.

Please describe if and how Respondent's proposed Solution meets this above prompt in the field below.

Tenable enhances vulnerability prioritization by integrating real-time threat intelligence from multiple sources, including internal expertise, vendor advisories among others. Its Predictive Prioritization feature analyzes over 150 data points to assign a Vulnerability Priority Rating (VPR), focusing remediation efforts on vulnerabilities most likely to be exploited within the next 28 days.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SLA: Uptime Guarantee: https://static.tenable.com/prod_docs/Service_Level_Agreement.pdf

Master Agreement, accepted via a click-thru acknowledgement at time of installation: https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L14 – Service Category 14: Cybersecurity Threat Intelligence (CTI)

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Cortex XSOAR

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide a response to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score.

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Cybersecurity Threat Intelligence (CTI) Solutions must aggregate threat data from multiple sources, analyze it to uncover emerging threats, and provide actionable intelligence to enhance security defenses. The Solution should integrate with an organization's existing security operations workflows, ensuring that threat intelligence is used to improve detection, prevention, and response efforts.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR helps security teams automate workflows, orchestrate response actions, and improve collaboration, and manage threat intelligence. Its ability to integrate with Cyber Threat Intelligence (CTI) sources enhances its capabilities in threat detection, response, and proactive security measures. XSOAR integrates CTI directly into its automation and orchestration workflows, allowing security teams to leverage threat intelligence to improve detection, incident response, and proactive defense strategies.

XSOAR automatically ingests and normalizes threat intelligence from various CTI sources. This eliminates the need for manual collection and processing of data, speeding up threat detection and response. The automation engine parses the data and turns raw intelligence into actionable information, i.e. creating alerts for known IOCs (e.g., IPs, URLs, file hashes), correlating it with internal security data, and triggering automated response workflows.

Once threat intelligence is ingested, XSOAR enriches security alerts with context from CTI. e.g., if a security incident involves a suspicious IP address, XSOAR can automatically query threat intelligence sources to see if that IP has been associated with any known malicious activity, e.g. botnet activity or malware distribution.

Cortex XSOAR automates response actions via playbook workflows based on threat intelligence. e.g., if CTI feed provides information on a newly discovered zero-day vulnerability, it can automatically trigger a patching process across the environment or block IP addresses associated with active exploitation of that vulnerability. XSOAR playbooks can be enhanced by integrating CTI into the decision-making process:

● Incident Response Playbooks: CTI triggers specific actions in an incident response workflow. If an alert is triggered by an IOC that matches a known threat actor, XSOAR could automatically escalate the severity, create a ticket, notify teams, and initiate additional investigation steps based on the threat intelligence.

● Threat Hunting Playbooks: Analysts can run automated queries based on threat intelligence feeds to proactively hunt for IOCs and tactics that align with specific threat actor behaviors.

● Incident Enrichment: If a potential threat is identified, XSOAR can call CTI services to gather context about threat actor TTPs, motivations, and targets, providing analysts with valuable insights for faster decision-making and response.

Integrating CTI into XSOAR platform improves the ability to detect, respond, and proactively manage threats. Automation of threat intelligence ingestion, enrichment, and response workflows, plus playbooks and incident response capabilities, enables faster, more informed security decisions. It can anticipate and mitigate emerging risks before they cause harm, making it a critical component in modern security operations.

For the portions that are prompts (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Threat Data Aggregation – Solution should include open-source threat feeds, paid subscriptions, and proprietary sources. The platform should support integration with standards-based threat intelligence feeds such as STIX, TAXII, and others.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR integrates with a wide array of threat intelligence sources, including open-source threat feeds, paid subscriptions, and proprietary sources. XSOAR supports 250+ threat feeds from providers like Crowdstrike, Mandiant, Unit 42, Microsoft, Recorded Future, etc. Most of these threat feeds are provided free, while some require a subscription from that provider. The platform supports integration with standards-based threat intelligence feeds eg STIX/TAXII.

Prompt 3: Threat Intelligence Platform (TIP) – Solution should consolidate and normalizes threat data, making it easy to share actionable intelligence with internal teams or external partners on a platform that has the capability to integrate with the CTI Solution. The platform should provide support for enrichment, scoring, and threat actor profiling.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSOAR functions as a TIP through its built-in Threat Intelligence Management (TIM) module, which consolidates and normalizes threat data from various sources, making it easy to share actionable intelligence with internal teams & external partners. XSOAR enrichment capabilities add contextual information to threat data, while scoring mechanisms prioritize threats based on their severity. Threat actor profiling enables the identification and tracking of TTPs.

Prompt 4: Real-Time Threat Alerts – Solution should notify Customer designated security teams of emerging threats relevant to their environment, such as new vulnerabilities, malware campaigns, or attack techniques in real-time. Alerts should include contextual information such as indicators of compromise (IoCs), threat actor motivations, and recommended mitigations.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSOAR ingests threat intelligence feeds, correlating indicators (IOCs, TTPs) with ingested alerts to detect emerging threats. Upon ingestion, XSOAR applies new indicators to historical and real-time alerts, triggering automated playbooks for incident response actions like enrichment, containment, and remediation based on the threat context. This proactive approach enables rapid response to emerging threats tailored to the organization's threat landscape.

Prompt 5: Custom Intel – Solution should include the ability to incorporate threat intelligence feeds and manual intelligence to include custom work/intel.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSOAR can integrate with custom threat intelligence, allowing organizations to integrate both automated threat intelligence feeds and manually curated intelligence. The platform supports the creation of custom IoCs tailored to the specific landscape of the Florida agency. Security teams can manually input their own threat data, create custom indicators, and define unique detection rules to enhance threat detection and response.

Prompt 6: Customer Feeds – Solution should include the ability to potentially change feeds if needed to include, remove, or modify research, analysis, and intelligence feeds.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSOAR provides a centralized platform where security teams can easily configure and adjust the threat intelligence feeds they rely on. Organizations can tailor their threat data landscape to meet their specific needs. Additionally, the Cortex XSOAR Marketplace provides access to numerous integrations, enabling seamless addition or modification of threat feeds.

Prompt 7: Integration with SIEM, SOAR, and SOC Tools – Solution should provide contextual threat intelligence directly within the security operations workflow. This integration should enable automated response actions such as blocking malicious IP addresses or adjusting firewall rules based on threat intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR seamlessly integrates with SIEM, SOAR, and other SOC tools to provide contextual threat intelligence directly within the security operations workflow. XSOAR also includes built-in SIEM capabilities for advanced event correlation and log management, as well as SOAR functionalities for orchestrating and automating response actions. XSOAR enables automated response actions which execute predefined remediation steps based on real-time threat intelligence.

Prompt 8: Feed Control – Solution should include Capabilities for incorporating premium feeds and manual intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR allows organizations to incorporate both premium threat intelligence feeds and manual intelligence seamlessly. XSOAR supports the integration of a wide range of premium threat intelligence feeds, ensuring that organizations can access high-quality, up-to-date threat data. XSOAR enables fine-grained control over which feeds are included, allowing for the addition, removal, or modification of threat intelligence sources as needed.

Prompt 9: Dynamic Threat Detection – Solution should include the ability to provide tailored threat intelligence focusing on specific threats relevant to an organization's unique environment, including industry-specific and organization specific risks and potential adversaries, ensuring that security measures are aligned with real-world scenarios.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR can provide tailored threat intelligence and security measures that are relevant to an agency's environment. There are several out-of-the-box playbooks available and these can be customized by SOC analysts or security admins to fit the agency's environment.

Prompt 10: Threat Context – Solution should include the ability to provide contextual awareness threat intelligence, to include custom intelligence, that provides insights that consider the broader context of an organization's operations, including user behavior, network architecture, and business priorities, allowing for more informed risk management.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR aggregates and enriches threat data from various sources, including custom intelligence. This enriched data provides insights that take into account the unique operational context, allowing for a more nuanced understanding of threats. XSOAR's advanced analytics and machine learning capabilities further enhance this contextual awareness by correlating threat data with user activities, network configurations, and critical business processes.

Prompt 11: Threat Insights – Solution should include capability to provide actionable insights from custom intelligence offering clear recommendations for mitigation, response strategies, and risk prioritization, empowering an organization to make informed decisions and improve their security posture effectively.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prompt 11 ResponsCortex XSOAR delivers actionable threat insights by enriching security events with custom intelligence via flexible integrations. Automated playbooks analyze, score, and prioritize alerts based on organizational risk profiles, triggering response actions and providing clear mitigation steps. This enables informed decisions and proactive security posture enhancement.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Service-Level Agreement

All capitalized terms not defined herein shall have the same meaning as set forth in the Palo Alto Networks End User Agreement.

Cortex XSIAM, XDR, XSOAR, and Xpanse-hosted services shall be available 99.9% of the time, measured monthly, excluding scheduled maintenance. Further, any downtime resulting from outages of third-party connections or utilities or other reasons beyond the control of Palo Alto Networks will be excluded.

Customer's sole and exclusive remedy and the entire liability of Palo Alto Networks, in connection with Cortex product service availability, shall be to credit customer 2% of monthly service fees (downtime credit) for each breach. A breach is defined as a period of 60 consecutive minutes of downtime (delays in data log ingestion are not considered downtime). Downtime shall begin to accrue as soon as customer notifies Palo Alto Networks that the service is down and will continue to accrue until service is restored.

In order to receive downtime credit, customers must notify Palo Alto Networks within 24 hours of service unavailability by initiating a help desk ticket. Failure to provide such notice forfeits the right to receive downtime credit. Such credits may not be redeemed for cash and shall not exceed one (1) week of service fees in any one (1) calendar month. Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate service under this Service-Level Agreement.

Palo Alto Networks will provide technical support based on the Customer Success Plan purchased:

- Under the Standard Plan, technical support is available via the Customer Support Portal.
- Under the Premium Plan, technical support is also available as above and by phone 24 hours per day, 7 days per week.

Customers may initiate a help desk ticket via support.paloaltonetworks.com. Palo Alto Networks will use commercially reasonable efforts to respond as follows:

Severity Level 1: Service is down; critically affects customer production environment. No workaround available yet. Standard: less than/equal to 2 hours; Premium: less than/equal to 1 hour

Severity Level 2: Service is impaired; customer production up, but impacted. No workaround available yet. Standard: less than/equal to 4 hours; Premium: less than/equal to 2 hours

Severity Level 3: A service function has failed; customer production not affected Support is aware of the issue and a workaround is available. Standard: less than/equal to 12 hours; Premium: less than/equal to 4 hours

Severity Level 4: Non-critical issue. Does not impact customer business. Feature, information, documentation, how-to, and enhancement requests from customer. Standard: less than/equal to 48 hours; Premium: less than/equal to 8 business hours

More Information

To learn more about Palo Alto Networks Support offerings, visit paloaltonetworks.com/support or contact your local account manager. For product information, visit paloaltonetworks.com/products.

Why Palo Alto Networks?

Palo Alto Networks is committed to your success in preventing successful cyberattacks. Our award-winning services and support organization give you timely access to technical experts and on- line resources to ensure your business is protected. We take our responsibility for your success seriously and continuously strive to deliver an exceptional customer experience. Our entire services organization and Authorized Support Centers are there to ensure maximum uptime and streamlined operations.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“Agreement”) GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term “Product” is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD

MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

"Affiliate" means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where "Control" means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks' use of all Palo Alto Networks Affiliates to deliver Products and Services.

"End User Data" means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

"Enterprise Program" means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

"Hardware" means hardware-based products listed on Palo Alto Networks' then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

"Product" means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

"Published Specifications" mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. "Software" means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

"Subscription(s)" means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced

Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according

to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED “AS IS”. PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L15 – Service Category 15: Data Security

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Prisma SASE_Strata Data Loss Prevention_Cortex

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Data Security Solutions are designed to protect sensitive information from unauthorized access, loss, or exfiltration. The Solution should monitor data in use, in motion, and at rest, enforcing data protection policies, and detecting any unauthorized attempts to access or share sensitive data. The Solution must integrate with existing security frameworks and support compliance requirements to ensure organizations meet their regulatory obligations.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Protecting Data-In-Motion and Data-At-Rest:

Data-in-motion must be protected while it traverses each point in the architecture regardless of location. Our solution can help the State protect data-in-motion on multiple levels, including encryption, malware prevention, DLP, access control, and continuous verification. At on-premise buildings, this is accomplished by leveraging our Next Gen Firewalls (NGFW) with Cloud Delivered Sec. Services (CDSS) to protect data before it's accessed & before it can leave the building.

One of the most important aspects of protecting data-in-motion is implementing a strong DLP solution at the boundary of each network enclave. Our NGFW provides a DLP service which can match over 1000 predefined patterns such as personally identifiable info. (PII), social security numbers, credit cards, bank account numbers, & more. These patterns are available out-of-the-box. The State can also leverage over 300 out-of-the-box ML patterns which can recognize contextual patterns for financial or personal info. Our DLP solution can also accept custom data patterns, which can be defined by the customer, to prevent other types of data loss that are specific to the State. These tailored, customizable patterns can be created on anything from custom source code to intellectual property. Most importantly, all of these checks can be performed consistently at every location and device to prevent the exfiltration of data, whether intentionally or unintentionally.

As application consumption switches to SaaS delivery model, it is critically important to protect data stored in SaaS applications. We offer a full CASB solution that protects cloud data that is accessed through SaaS methods. Our solution protects data from unauthorized access by checking for specific data patterns, malware attempts, and by leveraging ML to look at the contextual information in the data and categorize it. When data is requested, we execute a series of checks before allowing that information to be transmitted. The first step is identifying any patterns like social security numbers or credit card numbers to determine if that should be allowed. Next, we check for malicious intent using our WildFire technology to determine if the document is safe or contains malware. We leverage ML to understand the context of the data. Our ML detects & categorizes document as being either financial, legal, or healthcare documents. These types of documents are subject to various government regulations and standards. It's important to closely monitor these types of documents from the DLP perspective

Prisma Cloud Data Security Posture Management (DSPM) provides real-time visibility, control, & protection of data assets across any cloud & data store. It monitors cloud data stores closely and allows organizations to make security improvements, respond to data breaches immediately, attain compliance requirements and utilize flexible integrations.

For the portions that are prompts (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features..

Prompt 2: Data Discovery and Classification – Solution should automatically identify and classify sensitive data across the organization's infrastructure, including databases, file shares, cloud storage, and endpoint devices. The classification engine should apply tags based on predefined policies for data types such as Personally Identifiable Information (PII), financial data, and intellectual property. Enable continuous data discovery to detect new or modified data that requires protection.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Our SASE sets data access guidelines, enforcing least privilege to only auth. personnel access sensitive info; automatically apply labels to data at creation, regardless of where data is stored/utilized, so stringent controls protect sensitive info; reducing unauth. access & data leaks. Prisma Cloud DSPM, agentless, multi-cloud platform that continuously & automatically discovers, classifies, protects & governs sensitive data; w/custom classifiers to classify & tag.

Prompt 3: Data Loss Prevention (DLP) – Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

Please describe if and how Respondent's proposed Solution meets this prompt in the field below.

Our cloud-delivered DLP categorizes/protects data before it's exposed. Our enterprise DLP solution includes detection across: financial information, PII, SSN, credit cards, custom DLP expressions, regular expressions that identify/prevent release of custom content. DSPM w/real-time data detection & response (DDR), cloud DLP focusing on data protection in the cloud. DDR secures cloud data by leveraging ML algorithms, user behavior, access patterns & adv. log analytics.

Prompt 4: Encryption – Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

We protect data-at-rest: endpoint encryption, data access control, labeling, security brokering. We protect data-in-transit: DLP pattern matching algorithms, data obfuscation, and adv. network encryption w/quantum resistant ciphers. Our Post-Quantum tech integrates quantum-resistant algorithms to future-proof data against threats. DSPM monitors&alerts when sensitive data is shared/copied across geographies, insecure environments/entities granted with excessive access.

Prompt 5: User and Entity Behavior Analytics (UEBA) – Solution should analyze how users interact with sensitive data, detecting anomalous behaviors such as copying large amounts of data, accessing restricted files, or sharing data with unauthorized third parties. The Solution should use machine learning to identify insider threats and abnormal data access patterns before breaches occur.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XDR with IA for UEBA: The IA detects risky, malicious behavior, pinpoints attacks (credential theft, brute force & "the impossible traveler") detecting anomalies.IA has 360° user view of each user, user risk score, alerts, incidents.DSPM determines excessive access granted to individual entities comparing level of access w/actual usage, ML, applying policies & procedures, management access permissions across different cloud providers/data platforms.

Prompt 6: Automated Incident Response – Solution should automate response mechanisms to prevent unauthorized actions, such as blocking sensitive data transfers, issuing alerts, or requiring additional authentication when policy violations are detected. Quarantine suspicious files, block access to certain data, or alert security teams in real-time when DLP policies are breached.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Our NGFWs & Prisma SASE built-in DL leverages automation to prevent unauthorized actions, e.g. release of data. If potential policy violation is detected, our DLP tech prevents unauthorized release of data and creates a notification to alert security teams. We can integrate w/XSOAR: automated responses to notifications & disable access / quarantine users. DSPM integrates w/industry SOAR products including XSOAR.

Prompt 7: Audit Trails and Reporting – Solution should provide comprehensive audit trails of all data-related activities, including details of who accessed sensitive data, what actions were taken, and when. Generate detailed reports for compliance audits, security evaluations, and incident response investigations.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Our solution provides full audits, logging, reporting, and integration into Cortex XSIAM or other 3rd party tools. This integration includes forensics data capture, compliance w/audit standards, and incident response capabilities. Details regarding data related activities-User/Entity, Data Accessed, Actions, Time/Date are accessible through the Prisma Cloud console. Reporting consists of Security Reports (High Level), Compliance Reports (Detailed), and Alerts Reports.

Prompt 8: Compliance Management – Solution should integrate with compliance management platforms to help organizations meet regulatory requirements (e.g., GDPR, CCPA, HIPAA) and provide detailed reporting on data access and protection measures. Ensure organizations can map security controls to compliance frameworks and track any compliance gaps.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

We pursue compliance for the Federal and State government. standards & industry cert's: FedRAMP, StateRAMP, CJIS, CIS, HIPAA, others. Our security platforms include tools providing compliance reporting & tracking various compliance standards like CVEs. DSPM maps to compliance frameworks in the systems. SOC2, ISO 27001, GDPR, PCI, NIST. Prisma integrates with 3rd party systems via webhooks, pushing data, and via API for retrieving data from the systems.

Prompt 9: Data Catalog and Metadata Management – Solution should provide comprehensive data discovery, search, and metadata management across various data sources within the organization. Metadata management should include data definitions, lineage, quality metrics, and usage patterns to ensure full context for all data assets. Provide tools for data profiling to assess data quality, identify inconsistencies, and maintain data completeness.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Sensitive metadata is identified & protected: our DLP solution scans sensitive data (e.g. metadata) ensuring not exfiltrated, improperly accessed, metadata security. We integrate 3rd party data cataloging and metadata management, for comprehensive coverage. DSPM offers data classification for broad set of cloud assets & services; e.g. AWS, Azure & GCP for object, block storage, cloud DBs, DBaaS (Snowflake) & unmanaged databases.

Prompt 10: Integration with Data Management Tools – Solution should provide seamless integration with ETL (Extract, Transform, Load) tools, data warehousing, and analytics platforms to streamline data processing workflows. Ensure scalability, enabling the Solution to handle large volumes of data and grow with the organization's evolving needs.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Our security platforms provide seamless integration with big data toolsets, including data lakes, data warehouses, and big data analytics platforms. We can also provide log aggregation warehouses, combined with intelligent analytics capabilities that can handle large volumes of data at cloud scale. Prisma Cloud DSPM can integrate with any 3rd party system via webhooks as a push mechanism and via API calls for data that needs to be pulled.

Prompt 11: Master Data Management (MDM) – Solution should provide capabilities to create and maintain a single, consistent view of master data (e.g., customer, product, or supplier data) across the organization. Ensure high data quality through robust cleansing, deduplication, and validation tools, while supporting governance frameworks for data ownership and access control.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Palo Alto Networks DLP technologies and data insight tools integrate with the MDM capability to contribute to the unified view of master data.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

SERVICE LEVEL AGREEMENT

Prisma Cloud Subscription Service

Palo Alto Networks will use commercially reasonable efforts to make its Prisma Cloud SaaS Subscription service ("Service") meet 99.9% Monthly Uptime Availability as set forth herein ("Service Level"). In the unlikely event that Palo Alto Networks does not meet this Service Level commitment, Customers will be eligible to claim a service credit as described below ("Service Credit").

1. Service Level Commitment

Palo Alto Networks will use commercially reasonable efforts for the Service to maintain a Monthly Uptime Availability of at least 99.9%, which is calculated as follows:

Montly Uptime Availability Percentage = ((total time - downtime)/(total time)) x 100%

Total Time: Total number of minutes in a calendar month.

Downtime: Total number of minutes Customer lost external connectivity to the Prisma Cloud Console in a calendar month, excluding the number of minutes that meet the criteria under Section 2 - Exclusions.

2. Exclusions

Unavailability of the Service due to the following reasons shall be excluded from the Downtime, as provided for above:

2.1 Customer's equipment, networks, software, technology and/or third-party equipment, networks, software or technology (other than third-party equipment, networks, software or technology under Palo Alto Networks' control);

2.2 Failure of Customer's internet service provider, utility companies, or other vendor(s) Customer utilizes or relies on to access the Service and/or to access the internet;

2.3 Any reasonably unforeseeable interruption or degradation in Service due to actions or inactions caused by third parties or by activities outside Palo Alto Networks control, including, but not limited to, force majeure events;

2.4 Customer's failure to purchase adequate licenses to meet the volume or capacity at which it uses the Service, if the SLA would have been met if not for such failure;

2.5 Rightful suspension and/or termination by Palo Alto Networks of the Service pursuant to the Palo Alto Networks End User Licensing Agreement (www.paloaltonetworks.com/legal/eula), unless Customer and Palo Alto Networks have entered into a separate written agreement that specifically overrides such End User Licensing Agreement;

2.6 Any feature or portion of the Service marked or licensed to Customer as “Beta,” “Test,” “Preview,” or the like, indicating that the feature has not been made generally available (aka production);

2.7 Scheduled and unplanned maintenance windows;

2.8 High Availability events and scaling events.

2.9 Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate Service under this Service-Level Agreement.

3. Service Credit Claim

3.1 Service Credits. In the event that a Customer reasonably believes that the Service Level in connection with Customer’s use of the Service is not met in any calendar month, Customer may file a claim for Service Credit pursuant to Section 3.2 below. Once verified by Palo Alto Networks, Downtime shall begin to accrue from the time Customer notifies Palo Alto Networks pursuant to Section 3.2 and will continue to accrue until the Service is restored. Subject to the terms and conditions herein, for a qualified Claim, Palo Alto Networks will issue a Service Credit which equals to 2% of monthly Service fees when there is a period of at least sixty (60) consecutive minutes where Monthly Uptime Availability is not met, provided that: (1) no more than one Service Credit will be issued in any calendar day; and (2) for each calendar month, the maximum amount of Service Credit that Palo Alto Networks shall be liable for is one (1) week of the monthly Service Fee received by Palo Alto Networks.

3.2 Claims Process. Customers must have enrolled for an account on the Customer Support Portal in order to open a case and submit a Claim. If Customer believes it is entitled to a Service Credit, it must open a case on the Customer Support Portal (http://support.paloaltonetworks.com) within 24 hours of the start of the outage. When properly submitted, Palo Alto Networks will use commercially reasonable efforts to adjudicate claims promptly and in good faith based on its technical records and the information provided by the Customer. Customers may check on the Claim status at any time and may sign up to receive notifications when the Claim status changes. Adjudicated Claims shall be deemed final and may not be submitted again for re-consideration.

3.3 Claim Eligibility. To qualify to receive benefits under this Service Level Agreement, Customer must (a) be in good standing, i.e., Customer shall not be or have been delinquent in paying Service fees; and (b) have on-boarded the Service for at least sixty (60) days. This Service Level Agreement does not apply to trials or evaluations of the Service that are provided at no cost to the Customer.

4. Miscellaneous

4.1 Notifications. Customers may, at any time, obtain Service status updates at https://status.paloaltonetworks.com, which also provides region-specific status information and an alerts feature from which Customers may subscribe to receive Service notifications.

4.2 Applicability. The monthly Service fee attributable to the applicable Service excludes fees arising from additional services Customers may have purchased, such as Professional Services or consulting services, if any. The monthly Service fee may be calculated by dividing one-year Service fee by 12, three-year Service fee by 36, etc.

4.3 Distributor & Reseller Orders. If a Customer has purchased the Service through an authorized Palo Alto Networks distributor or reseller, the Service Credit will be made to the distributor which placed the order for the Service. Distributors are responsible for reimbursing the reseller which in turn will credit the Customer. If a Customer purchased the Service directly from Palo Alto Networks, then Palo Alto Networks shall issue the Service Credit towards the next renewal of the Service.

4.4 Entire Liability. The foregoing terms state Palo Alto Networks' sole and exclusive liability and Customer's sole and exclusive remedy for any Claim of non-compliance of this Service Level Agreement.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("Agreement") GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term "Product" is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS "CUSTOMER", "END USER", "YOU" or "YOUR") AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS "PALO ALTO NETWORKS").

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose ("Evaluations"), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

“Affiliate” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Services.

“End User Data” means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

“Enterprise Program” means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

“Hardware” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“Product” means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

“Published Specifications” mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. “Software” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“Subscription(s)” means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

“Systems Data” means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED “AS IS”. PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks’ suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks’ suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the

Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L15 – Service Category 15: Data Security

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Rubrik Security Cloud and Data Security Posture Management (DSPM)

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Data Security Solutions are designed to protect sensitive information from unauthorized access, loss, or exfiltration. The Solution should monitor data in use, in motion, and at rest, enforcing data protection policies, and detecting any unauthorized attempts to access or share sensitive data. The Solution must integrate with existing security frameworks and support compliance requirements to ensure organizations meet their regulatory obligations.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik is on a mission to secure the world's data. Rubrik pioneered Zero Trust Data Security to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. The foundation of the solution is Rubrik's proprietary, append-only file system that prevents the modification and deletion of data so that it is readily available for recovery. Rubrik's breadth of data security capabilities are delivered in a single, integrated solution, and includes:

- logical air gap technology so data cannot be discovered, accessed, or modified by unauthorized users
- immutable file system: once written, the data cannot be modified, encrypted, or deleted
- advanced authentication: customizable RBAC, SAMF support, MFA, TOTP with granular role-based access control
- prevent unauthorized disclosure of data, at-rest and in-transit, using strong encryption
- ransomware detection and investigation to discover data anomalies
- incident containment to prevent malware reinfection
- orchestrated application recovery to aid teams to restore in hours, not weeks

Rubrik's latest threat hunting capabilities allow organizations to directly scan backups for indicators of compromise (IOC), including ransomware. With this added intelligence, agencies can more accurately identify the last known clean copy of data in order to prevent reinfection during and after recovery.

Rubrik DSPM (Data Security Posture Management) and SDM (Sensitive Data Monitoring) provide comprehensive visibility into where sensitive data lives in the environment and who has access to it, which is crucial to reducing data exposure and exfiltration risks. It can discover, classify, and report on sensitive data without any impact to production. DSPM provides proactive insight into a company's sensitive data to protect from exfiltration. This can be utilized alongside Rubrik's comprehensive data protection and recovery services to provide a compelling end-to-end data cyber resilience strategy. Rubrik finds and classifies your sensitive and regulated data across on-premises, cloud, and SaaS environments, and so you can put security controls in place and reduce the risk of data theft. DSPM ensures that sensitive data is not stored in unauthorized locations, such as lower environments or unauthorized geo-locations. These policies help you keep track of data that is moving between accounts and borders and ensure that sensitive data is only stored where it is allowed. SDM can also pass information about the sensitive data that has been discovered via APIs to industry leading security solutions (such as, Zscaler and Palo Alto Networks) to further strengthen an organziation's overall security posture.

For the portions that are prompts (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features..

Prompt 2: Data Discovery and Classification – Solution should automatically identify and classify sensitive data across the organization's infrastructure, including databases, file shares, cloud storage, and endpoint devices. The classification engine should apply tags based on predefined policies for data types such as Personally Identifiable Information (PII), financial data, and intellectual property. Enable continuous data discovery to detect new or modified data that requires protection.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Prompt 2 Rubrik's cloud-native Data Security Posture Management (DSPM) solution continuously discovers and classifies all cloud data, structured and unstructured, across managed and self-hosted data stores, without the data ever leaving your environment. It analyzes access, usage patterns, and security posture, and provides actionable, guided remediation for data security risks. Easily ensures all data is properly owned and tagged to fast-track evidence collection.Goes Here

Prompt 3: Data Loss Prevention (DLP) – Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

Please describe if and how Respondent's proposed Solution meets this prompt in the field below.

Rubrik DSPM finds and classifies your sensitive and regulated data across on-premises, cloud, and SaaS environments, so you can put security controls in place and reduce the risk of data theft. Also, Rubrik SDM can pass sensitive data analysis info to DLP Solutions (such as, Zscaler) via APIs to prevent that sensitive data from being exposed.

Prompt 4: Encryption – Solution should monitor and block unauthorized sharing of sensitive data across multiple communication channels, including email, cloud services, USB devices, and other pathways. Ensure that sensitive data is protected from being copied or moved without proper authorization, with real-time monitoring and alerting capabilities.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik DSPM finds and classifies your sensitive and regulated data across on-premises, cloud, and SaaS environments, so you can put security controls in place and reduce the risk of data theft. Also, Rubrik SDM can pass sensitive data analysis info to DLP Solutions (such as, Zscaler) via APIs to prevent that sensitive data from being exposed.

Prompt 5: User and Entity Behavior Analytics (UEBA) – Solution should analyze how users interact with sensitive data, detecting anomalous behaviors such as copying large amounts of data, accessing restricted files, or sharing data with unauthorized third parties. The Solution should use machine learning to identify insider threats and abnormal data access patterns before breaches occur.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik DSPM reduces data exposure and identities risk by detecting excessive and misconfigured permissions. It can identify all internal and external users, roles, and resources with access to sensitive data. Then, admins can monitor and control each user's access to sensitive data based on their roles and responsibilities. This process ensures that only authorized users have access to sensitive assets. Rubik DSPM leverages Dynamic ML models usage telemetry to deliver low false positives.

Prompt 6: Automated Incident Response – Solution should automate response mechanisms to prevent unauthorized actions, such as blocking sensitive data transfers, issuing alerts, or requiring additional authentication when policy violations are detected. Quarantine suspicious files, block access to certain data, or alert security teams in real-time when DLP policies are breached.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik DSPM data detection and response (DDR) solution lets you detect data breaches as they occur and quickly contain active threats to minimize damage. DSPM identifies anomalous data access and behavior — alerting you on data exfiltration, suspicious third-party access, insider threats, accidental data leaks, data misuse, and other threats. It finds data threats that other solutions do not detect.

Prompt 7: Audit Trails and Reporting – Solution should provide comprehensive audit trails of all data-related activities, including details of who accessed sensitive data, what actions were taken, and when. Generate detailed reports for compliance audits, security evaluations, and incident response investigations.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik is SOC II Type 2 certified, which guarantees its capacity to safeguard sensitive and proprietary information. Rubrik prioritizes the security and confidentiality of clients, employing established protocols and frameworks to ensure the protection of data. All activity is captured and secured in the audit logs. Centralized reporting with drill down views is included.

Prompt 8: Compliance Management – Solution should integrate with compliance management platforms to help organizations meet regulatory requirements (e.g., GDPR, CCPA, HIPAA) and provide detailed reporting on data access and protection measures. Ensure organizations can map security controls to compliance frameworks and track any compliance gaps.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

DSPM integrates seamlessly with your existing workflows, and can integrate with CSPMs, enterprise data catalogs, ITSM and SIEM tools, team communication services, and privacy and governance management tools via APIs. The platform also supports multiple CSPs and data warehouses like AWS, Azure, GCP, and Snowflake. It can detect and remediate violations of data privacy regulations and industry standards (GDPR, PCI DSS, etc.), then generate audit-ready reports.

Prompt 9: Data Catalog and Metadata Management – Solution should provide comprehensive data discovery, search, and metadata management across various data sources within the organization. Metadata management should include data definitions, lineage, quality metrics, and usage patterns to ensure full context for all data assets. Provide tools for data profiling to assess data quality, identify inconsistencies, and maintain data completeness.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik DSPM can read from multiple data sources (such as, databases, data pipelines, object storage, disk storage, managed file storage, data warehouses, and lakes) across cloud environments and datacenters. Multi-step, intelligent classification evaluates the context of the data type to ensure accuracy and low false positives. Data discovery and clasification is a dynamic and ongoing process.

Prompt 10: Integration with Data Management Tools – Solution should provide seamless integration with ETL (Extract, Transform, Load) tools, data warehousing, and analytics platforms to streamline data processing workflows. Ensure scalability, enabling the Solution to handle large volumes of data and grow with the organization's evolving needs.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik DSPM functions across multi-cloud environments, extending to all major cloud service providers. It can read from various databases, data pipelines, object storage, disk storage, managed file storage, data warehouses, lakes, and analytics pipelines (S3 buckets, BigQuery, Redshift, Storage Container, EBS, RDS, DynamoDB, etc.) both managed and self-hosted. It can classify sensitive data in structured, semi-structured, and unstructured formats.

Prompt 11: Master Data Management (MDM) – Solution should provide capabilities to create and maintain a single, consistent view of master data (e.g., customer, product, or supplier data) across the organization. Ensure high data quality through robust cleansing, deduplication, and validation tools, while supporting governance frameworks for data ownership and access control.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Rubrik DSPM monitors constantly changing data structures and storage locations throughout the organization, ensuring that the data security team always has a unified view of all sensitive, proprietary and regulated data assets. This data-centric policy framework ensures that we're addressing all categories of sensitive data violations and promotes good data hygiene practices, making it easier to maintain compliance and protect your organization's sensitive data.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

RUBRIK SERVICE LEVEL AGREEMENT

This Rubrik Service Level Agreement ("SLA") sets out the terms governing Rubrik's Service Level Agreement for the Rubrik Service and forms part of the Agreement. Capitalized terms not defined herein are as defined in the Agreement.

1. SERVICE COMMITMENT.

1.1 During the applicable Subscription Period, Rubrik will use commercially reasonable efforts to maintain a service login availability to the Rubrik Service of 99.9% per each calendar month (the "Service Commitment"). Customers can view Rubrik's current uptime status at https://status.rubrik.com. The Service Commitment does not include Downtime. The Rubrik Service uptime is calculated as the total number of minutes the Rubrik Service is available to Customer in the applicable month divided by the total number of minutes that month, minus Downtime. In the event the Rubrik Service does not meet the Service Commitment, Customer shall become entitled to the Service Credit specified in the table set out below, after submitting a written claim for such Service Credit as outlined in Section 3 (Claiming a Service Credit), provided that Customer is in compliance with the terms of the Agreement. Provision of a Service Credit by Rubrik is Customer's sole and exclusive remedy for any failure by Rubrik to meet the Service Commitment.

1.2 The Service Commitment does not apply to: (i) Free Trials; (ii) unavailability caused by any unauthorized action or lack of action when required from Customer, or anyone authorized by Customer, or otherwise resulting from Customer's failure to follow appropriate security practices; (iii) unavailability caused by factors outside Rubrik's reasonable control, including but not limited to a Force Majeure event or failure of a cloud service provider; (iv) unavailability that results from the use of services or software not provided by Rubrik, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services; and (v) Customer's violation of the Agreement, including the AUP.

2. SERVICE CREDITS.

Monthly Service Login Availability Percentage	Service Credit
Less than 99.9% but greater than or equal to 99.0%	3 days of additional Rubrik Service
Less than 99.0% but greater than or equal to 95.0%	7 days of additional Rubrik Service
Less than 95.0%	30 days of additional Rubrik Service

Service Credits shall be provided as an additional number of days of the affected portion of the Rubrik Service, applied upon renewal of the applicable Subscription Period, without any additional fees payable by Customer. Rubrik shall not in any circumstances be obligated to pay any money or issue any refund to the Customer.

3. CLAIMING A SERVICE CREDIT. In order to receive a Service Credit, Customer must submit a claim by raising a support case with Rubrik's support team within thirty (30) days after the end of the calendar month during which the Service Commitment was not met, detailing the calendar month for which Customer is claiming the Service Credit together with the dates and times of when the Service Commitment was not met. Rubrik may require Customer to provide further information to support its claim for a Service Credit. If Customer fails to provide such information, Rubrik may reject Customer's request for a Service Credit. If Rubrik finds that Customer is eligible for a Service Credit, it will notify Customer of the same within a reasonable time period of receiving all requested information from Customer. The aggregate maximum number of Service Credits that can be issued to Customer shall not exceed two (2) months of Rubrik Service in any single year of a Subscription Period.

SERVICE AGREEMENT

IMPORTANT: READ THIS RUBRIK SERVICE AGREEMENT ("AGREEMENT") BEFORE INSTALLING OR USING THE RUBRIK SERVICE (AS DEFINED BELOW). THIS IS A LEGAL AGREEMENT BETWEEN RUBRIK, INC. ("RUBRIK") AND YOU OR THE ENTITY THAT YOU REPRESENT ("CUSTOMER") (INDIVIDUALLY A "PARTY", COLLECTIVELY THE "PARTIES"). THIS AGREEMENT GOVERNS CUSTOMER'S USE, INCLUDING ANY FREE TRIAL USE, OF THE RUBRIK SERVICE (AS DEFINED BELOW). BY ACCEPTING THIS AGREEMENT, EITHER BY CLICKING A BOX OR BUTTON INDICATING YOUR ACCEPTANCE, BY EXECUTING AN ORDER THAT REFERENCES THIS AGREEMENT, OR BY DOWNLOADING, INSTALLING, USING OR ACCESSING THE RUBRIK SERVICE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE DOWNLOADING, INSTALLING, USING OR ACCESSING THE RUBRIK SERVICE FOR USE BY AN ENTITY OR OTHER INDIVIDUALS OTHER THAN YOURSELF, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THIS AGREEMENT. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT COPY, INSTALL, USE OR ACCESS THE RUBRIK SERVICE.

1. DEFINITIONS.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. For purposes of this definition, "control" means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.

"Business Contact Data" means the names, addresses, telephone numbers and all other business-related information of each Party's personnel, that may be collected or exchanged between the Parties in the ordinary course of maintaining the business relationship, such as contract management, sales and ordering, and business development.

"Customer Data" means Customer's content and application data uploaded by or on behalf of Customer to the Rubrik Service for backup and recovery.

"Customer Personal Data" means Customer Data that is Personal Data owned or controlled by Customer and which Rubrik, a Rubrik Affiliate or Subprocessor (as defined in the Data Processing Addendum ("DPA")) may process in the course of providing the Rubrik Service.

“Documentation” means the Rubrik Licensing Guide available to Customer at the Rubrik Site, and the Rubrik Service user guides available to Customer within the Rubrik Service user-interface and on the Rubrik support portal.

“Downtime” means, either: (i) a scheduled period of time for maintenance and upgrade activity during which the Rubrik Service is not available to Customer; or (ii) unannounced periods of time for emergency maintenance and upgrade activity during which the Rubrik Service is not available to Customer.

“Effective Date” means the date Customer accepts the terms of this Agreement.

“Non-Rubrik Application” means web-based, offline, mobile, or other software that originates from Customer or a third party and interoperates with the Rubrik Service.

“Order” means the purchase order or other agreed upon legally binding document placed by Customer which specifies the Subscription Period, quantities, and description of the Rubrik Service, Support Services and/or Professional Services purchased by Customer from a Rubrik authorized reseller (“Reseller”).

“Personal Data” means (i) any information relating to an identified or identifiable natural person; and/or (ii) any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Unless prohibited or specifically governed by Data Protection Laws (as defined in the DPA), Personal Data shall not include information or data that is anonymized, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.

“Professional Services” means the implementation, configuration, and training services purchased by Customer under an Order.

“Rubrik Service” means the Rubrik cloud-based SaaS offering purchased by Customer as specified in an applicable Order. The Rubrik Service includes Rubrik offline software components described in the Documentation (if applicable) and all updates, copies, modifications, and derivative works thereof. The Rubrik Service excludes Free Trials and Non-Rubrik Applications.

“Rubrik Site” means the Rubrik legal page at https://www.rubrik.com/legal.

“Term” means the period of time from the Effective Date until the last Subscription Period expires.

2. ACCESS GRANT.

2.1 Right to Use the Rubrik Service. Subject to Customer’s compliance with the terms and conditions of this Agreement and Customer’s payment of all fees due, for the duration of the applicable Subscription Period, Rubrik grants Customer a limited, non- exclusive, non-sublicensable, non-transferable (except as expressly permitted herein) revocable, right to access and use the Rubrik Service in accordance with the Documentation, solely for Customer’s internal business purposes, limited to the quantities and any other limitations set forth in the applicable Order. To the extent that use of the Rubrik Service requires Customer to install Rubrik software components, for the duration of the Subscription Period, Rubrik grants Customer a limited, revocable, non-exclusive, non-transferable, non-sublicensable license to use the object code form of such software solely for Customer’s internal business purposes in accordance with the Documentation and in connection with Customer’s use of the Rubrik Service. Customer may use the Rubrik Service for the benefit of its Affiliates, and Affiliates may use the Rubrik Service for their own benefit, limited to the quantities and any other limitations as set forth in the applicable Order and subject to compliance with all terms of this Agreement. Customer guarantees that each Affiliate will fully perform its obligations hereunder, and Customer is responsible for any breach of this Agreement by its Affiliates. Rubrik will use commercially reasonable efforts to provide consistent site availability for the Rubrik Service during the applicable Subscription Period in accordance with Exhibit A (Rubrik Service Level Agreement). Notwithstanding anything to the contrary in this Agreement, any use of the Rubrik Service by Customer or its users in breach of the Acceptable Use Policy ("AUP") or applicable law or that threatens the security, integrity or availability of the Rubrik Service (in Rubrik's reasonable judgment) may result in the immediate suspension of Customer's access to the Rubrik Service; however, Rubrik will use commercially reasonable efforts to provide Customer with notice and an opportunity to remedy such breach or threat prior to such suspension. If Customer's access is suspended, Rubrik will restore access promptly after Customer remedies the breach. During the applicable Subscription Period, Rubrik will provide Support Services purchased under an applicable Order to Customer as set forth in Rubrik's then-current support terms found at the Rubrik Site.

2.2 Subscription Period; Term of Agreement. Subject to Section 3 (Customer Obligations) Customer may use the Rubrik Service for the duration of Customer's subscription specified in the applicable Order ("Subscription Period"). If Customer does not renew the subscription to the Rubrik Service on or before the Subscription Period renewal date, Customer's right to use the Rubrik Service terminates and the Rubrik Service will no longer operate. The Agreement will remain in effect for the Term.

3. CUSTOMER OBLIGATIONS. Customer's use of the Rubrik Service is subject to the AUP found at the Rubrik Site. Customer will not, nor will Customer assist others to: (i) copy or distribute the Rubrik Service or Documentation (except for a reasonable number of copies of the Documentation for internal use) or modify, encumber, enhance or create any derivative works of the Rubrik Service or Documentation, including without limitation, customization, translation or localization; (ii) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or the underlying ideas, algorithms, structure, sequence and organization of the Rubrik Service; (iii) sell, license, sublicense, rent, lease, lend or transfer the Documentation or Rubrik Service or provide, disclose or use the Rubrik Service or Documentation for the benefit of any third party, including but not limited to timesharing or service bureau purposes;

(iv) remove, alter or obscure any patent, copyright, trademark or other proprietary notices on the Rubrik Service or Documentation; (v) publish or disclose to any third party any technical features or specifications, performance, functionality, or benchmark tests, or comparative or competitive analyses relating to the Rubrik Service and Free Trials unless expressly authorized in writing in advance by Rubrik; (vi) access or use the Rubrik Service or Documentation to promote, distribute, sell, or support any product or service competitive with Rubrik; (vii) violate or circumvent any technological restrictions in the Rubrik Service; (viii) use the Rubrik Service for any purpose or in any manner not authorized by this Agreement (including, without limitation, for any purpose competitive with Rubrik); (ix) use the Rubrik Service in violation of any applicable local, federal, or other laws and regulations; or (x) host, support, use or otherwise deploy the Rubrik Service as a service on behalf of any unaffiliated third party without Rubrik's express written agreement. Customer must promptly notify Rubrik of any unauthorized use of or access to the Rubrik Service purchased by Customer. Customer is responsible for using a key management system for secure storage of Customer's encryption keys. Customer acknowledges and agrees that Rubrik is unable and has no obligation to recover Customer’s access credentials or encryption keys (“Credentials”) if lost by the Customer. Customer acknowledges the loss of such Credentials by Customer may result in the loss of access to Customer Data. Customer is responsible for maintaining the confidentiality of all usernames and passwords required for its use of and access to the Rubrik Service and for all activities conducted in connection therewith.

4. PROPRIETARY RIGHTS.

4.1 Customer Data. As between Rubrik and Customer, Customer owns Customer Data. Customer grants to Rubrik, its Affiliates and applicable Subprocessors a worldwide, limited-term license to host, copy, transmit and display Customer Data, as reasonably necessary for Rubrik to provide the Rubrik Service in accordance with this Agreement. Subject to the limited licenses granted herein, Rubrik acquires no right, title or interest in or to any Customer Data. Customer shall be responsible for the accuracy, quality and legality of Customer Data and the means by which Customer acquired Customer Data.

4.2 Rubrik Service. As between Rubrik and Customer, Rubrik and its licensors retain all rights, title, and interest in and to the Rubrik Service, Documentation, Support Services and Professional Services, including all copies, modifications, and derivative works thereof and all intellectual property rights therein. Rubrik grants to Customer a worldwide, non-exclusive, non-transferable, non-sublicensable right to use the Support Services and/or Professional Services solely for Customer’s use with the Rubrik Service during the applicable Subscription Period. This Agreement does not grant Customer any rights not expressly set forth herein. Customer may elect to provide suggestions, requests for enhancements or functionality, or other feedback to Rubrik relating to the operation of the Rubrik Service (“Feedback”). If Customer, in its sole discretion, provides Feedback, Customer hereby grants Rubrik a royalty-free, worldwide, transferable, sublicensable, irrevocable, perpetual license to use or incorporate into its products and services any Feedback as it sees fit without obligation or restriction of any kind. Customer can access any notice and attribution files for any applicable open-source software distributed with, hosted with, provided with or otherwise made use of with the Rubrik Service on the Rubrik support portal.

5. ORDERS; FEES. Customer will purchase the Rubrik Service, Support Services and/or Professional Services from a Reseller pursuant to a separate agreement between Customer and such Reseller (“Partner Agreement”). Customer shall pay the Reseller all amounts due and owing under an Order (along with all taxes, tariffs, and duties) in accordance with the Partner Agreement. The Partner Agreement is between Customer and Reseller and is not binding on Rubrik. In the event Customer places an Order in a third-party cloud marketplace in which Rubrik has agreed to participate, Customer is responsible for payment of all fees (along with all taxes, tariffs and duties) in accordance with the terms of the Order placed in such cloud marketplace, and the marketplace is deemed to be the Reseller for purposes of the Order.

6. VERIFICATION. During the Term and for a period of one (1) year thereafter, Rubrik (or its independent third-party auditors) has the right, upon reasonable notice, to reasonably audit Customer’s relevant systems and records to confirm Customer’s compliance with this Agreement. Rubrik may conduct no more than one (1) audit per twelve (12) month period and Customer shall reasonably cooperate with Rubrik (or its independent third-party auditors) for such audit. Rubrik shall conduct such audit during Customer’s regular business hours and in a way designed to minimize business disruption. If an audit discloses Customer has installed, accessed, used, or otherwise permitted use of or access to the Rubrik Service in a manner that is not expressly

permitted by this Agreement, Customer agrees to promptly reimburse the applicable Reseller, or Rubrik, for any unpaid fees for such use or access to the Rubrik Service.

7. RESERVED

8. CONFIDENTIALITY. Customer and Rubrik may disclose Confidential Information to each other during the Term. “Confidential Information” means all nonpublic proprietary business and technical information disclosed by one Party (“Disclosing Party”) to the other Party (“Receiving Party”) which is in tangible form and labeled “confidential” or the like, or that reasonably should be understood to be confidential given the circumstances of disclosure and the nature of the information. Confidential Information includes, but is not limited to, the Rubrik Service, Documentation, Free Trials, strategic roadmaps, product plans, product designs and architecture, technology and technical information, security processes, security audit reviews and business and marketing plans. Confidential Information will not include information that: (i) was already in Receiving Party’s possession without confidentiality obligations; (ii) is rightfully received by Receiving Party without confidentiality obligations; (iii) is independently developed by the Receiving Party without use of or reference to the Disclosing Party’s Confidential Information as supported by documents and other competent evidence; or (iv) is in the public domain without breach of a confidentiality obligation by the Receiving Party as supported by documents and other competent evidence. The Receiving Party will protect Confidential Information received from the Disclosing Party using the same degree of care as it uses to protect its own similar confidential materials, but in no event using less than reasonable care. The Receiving Party will disclose Confidential Information only to its employees, Affiliates, alliance partners or subcontractors (as applicable) who have a need to know for purposes of this Agreement and who are under a written obligation of confidentiality no less protective than this Agreement. Each Party may also disclose Confidential Information, including the terms and conditions of this Agreement, in confidence to its legal counsel, accountants, auditors, banks and financing sources, and their advisors. Confidential Information may be disclosed in response to a subpoena or order of a court or governmental agency, provided however, that if not otherwise prohibited, the Receiving Party will notify the Disclosing Party promptly of such disclosure to enable the Disclosing Party to seek an appropriate protective order. The Parties’ obligations with respect to Customer Data are set forth in Section 9 (Security; Protection of Customer Data). Upon expiration or termination of this Agreement for any reason, the Receiving Party will, upon request, return or destroy the Disclosing Party’s Confidential Information. Notwithstanding the foregoing, the Receiving Party may retain copies of Disclosing Party’s Confidential Information stored electronically on data archives or back-up systems or to comply with the laws or regulations applicable to the Receiving Party, provided that such copies shall at all times be subject to the terms of this Agreement while in Receiving Party’s possession or control.

9. SECURITY; PROTECTION OF CUSTOMER DATA. Rubrik will implement and maintain commercially reasonable administrative, physical and technical safeguards and measures designed to address the security, confidentiality and availability of Customer Data in the Rubrik Service as more fully set forth in the Data Security Schedule and the DPA, both of which are available at the Rubrik Site.

10. PROFESSIONAL SERVICES AND PROFESSIONAL SERVICES WARRANTY. Customer may place an Order for Professional Services. Professional Services may be performed by Rubrik or subcontractors acting on Rubrik’s behalf. In regard to Professional Services, Rubrik warrants that: (i) it and its personnel have the necessary knowledge, skills, experience, qualifications and

resources to provide and perform the Professional Services; and (ii) the Professional Services will be performed in a professional and workmanlike manner in accordance with industry standards. As a condition to Rubrik providing Professional Services hereunder, Customer shall: (a) provide good faith cooperation and access to such information, facilities, and equipment as may be reasonably required in order to provide the Professional Services; and (b) provide such personnel assistance as may be reasonably requested from time to time. If, through no fault or delay by Customer, or any failure by Customer or Customer's representatives to perform in accordance with this Section 10 (Professional Services and Professional Services Warranty), the Professional Services do not conform to the foregoing warranty, and Customer notifies Rubrik within ten (10) days of Rubrik's completion of the Professional Services, Rubrik will re-perform the non-conforming portion(s) of the Professional Services at no additional cost to Customer. Unless otherwise agreed upon by the Parties in writing, the obligation of Rubrik to provide Professional Services to the Customer expires the earlier of: (i) completion of the Professional Services; or (ii) six (6) months from the date Rubrik accepts the applicable Order for the Professional Services. Credit for any unused Professional Services will not be transferable to any other services.

11. WARRANTIES AND DISCLAIMER.

11.1 Rubrik Service Warranty. Rubrik warrants to Customer during the applicable Subscription Period ("Warranty Period") that the Rubrik Service will conform in all material respects to the applicable Documentation ("Rubrik Service Warranty").

11.2 Remedy; Exclusions. Rubrik's sole obligation under the Rubrik Service Warranty, and Customer's exclusive remedy, is to use commercially reasonable efforts to correct the non-conformity during the Warranty Period. If Rubrik is not able to correct the non-conformity in the Rubrik Service such that it complies with the Rubrik Service Warranty, Rubrik will process a refund of the unused, prepaid fees for such non-conforming Rubrik Service via the applicable Reseller and Customer's right to use the Rubrik Service for which the refund was processed terminates. Customer's obligation is to provide all information reasonably requested to enable Rubrik to cure any such deficiencies. The foregoing warranties do not apply to the Rubrik Service: (i) that is installed, operated, maintained, stored or used improperly, or in any manner not in accordance with the Documentation, this Agreement or Rubrik's written instructions; (ii) that is repaired, altered or modified other than by Rubrik or its authorized service provider; or (iii) where the issue is caused by any failure of third-party software or cloud services not supplied by Rubrik.

11.3 Disclaimer of Warranties. EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. FREE TRIALS ARE PROVIDED "AS IS," AND AS AVAILABLE, EXCLUSIVE OF ANY WARRANTY OR INDEMNITY WHATSOEVER.

12. INDEMNIFICATION.

12.1 Indemnification by Rubrik. Rubrik agrees to defend or settle, at Rubrik's expense, a third-party claim or cause of action against Customer alleging with specificity that, standing alone, the Rubrik Service or its use: (i) infringes a U.S., European Economic Area, or U.K. copyright or patent of such third party; or (ii) infringes all inventive aspects of a U.S., European Economic Area, or U.K. patent of such third party ("Claim") and to pay damages finally awarded against Customer by a court of competent jurisdiction or as agreed to in a settlement. Rubrik's obligations hereunder do not apply with respect to any Claim that arises out of: (a) any unauthorized use, reproduction or distribution of the Rubrik Service; (b) allegations of infringement that could have been asserted without Customer's use of the specific Rubrik Service, for example, allegations arising from Customer's use of an industry standard (e.g., logging in with password, or using standard encryption) ; (c) the Rubrik Service being modified after delivery without Rubrik's prior written authorization; or (d) Customer's continued use of the allegedly infringing Rubrik Service after Rubrik modified the Rubrik Service to be non-infringing. If any Claim arises, Rubrik may, at its sole option and expense: (A) replace or modify the affected Rubrik Service to make it non-infringing;

(B) procure a license for Customer's continued use of the affected Rubrik Service; or if Rubrik determines (in its sole discretion) that (A) and (B) are not commercially viable, terminate Customer's rights thereto, in which case Rubrik will process a pro-rated refund for the applicable prepaid unused fees for such Rubrik Service covering the remainder of the applicable Subscription Period via the applicable Reseller. This Section 12.1 (Indemnification by Rubrik) states Customer's sole and exclusive remedy, and Rubrik's sole liability, with respect to infringement of third-party intellectual property rights.

12.2 Customer Indemnity. Customer agrees to defend or settle, at Customer's expense, a third-party claim or cause of action against Rubrik alleging that Customer's provision or use of Customer Data violates a third party's rights, and to pay damages finally awarded against Rubrik by a court of competent jurisdiction or as agreed to in a settlement..

12.3 Indemnification Process. As a condition of receiving indemnity as described in this Section 12 (Indemnification), the Party seeking the indemnity will provide the other Party with: (i) prompt written notice of the claim, provided, however, that the failure to give such notice shall not relieve the indemnifying Party of its obligations hereunder except to the extent that the indemnifying Party is prejudiced by such failure; (ii) complete control over the defense and settlement of the claim, provided that the indemnifying Party will not settle any claim without the other Party's prior written permission if the settlement fails to unconditionally release the indemnified Party from all liability pertaining to the claim (such permission not to be unreasonably withheld, delayed or conditioned); and (iii) reasonable assistance in connection with the defense and settlement of the claim.

13. LIMITATION OF LIABILITY.

13.1 Disclaimer of Consequential Damages. EXCEPT FOR CUSTOMER'S VIOLATION OF RUBRIK'S INTELLECTUAL PROPERTY RIGHTS, IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUE, LOSS OR CORRUPTION OF DATA OR THE COST OF COVER, HOWEVER CAUSED, WHETHER BASED IN CONTRACT, TORT, WARRANTY, NEGLIGENCE, INDEMNITY OR ANY OTHER THEORY OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES. IN SUCH AN EVENT, THIS EXCLUSION WILL NOT APPLY TO THE EXTENT THE EXCLUSION IS PROHIBITED BY LAW.

13.2 Limitation of Liability. IN NO EVENT WILL RUBRIK'S, ITS AFFILIATES' AND ITS LICENSORS' TOTAL, CUMULATIVE AND ENTIRE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL FEES PAID BY CUSTOMER FOR THE RUBRIK

SERVICE GIVING RISE TO THE LIABILITY FOR THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE (OR, THE FEES PAID OR PAYABLE FOR THE FIRST 12 MONTHS OF THE SUBSCRIPTION PERIOD, IF LESS THAN 12 MONTHS HAVE ELAPSED). THE FOREGOING LIMITATION SHALL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY OR ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY HEREIN BUT WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

14. TERMINATION.

14.1 Termination for Cause. Any Orders placed pursuant to this Agreement are non-cancellable and non-refundable, except as provided for herein. Notwithstanding the foregoing, a Party may terminate this Agreement if the other Party: (i) materially breaches this Agreement and such breach is not cured within thirty (30) days of such Party's receipt of written notice describing the breach; or (ii) becomes insolvent, admits in writing of its inability to pay its debts as they mature, makes an assignment for the benefit of creditors, becomes subject to control of a trustee, receiver or similar authority, or becomes subject to any bankruptcy or insolvency proceeding.

14.2 Post-Termination Obligations. Upon expiration or termination of this Agreement, including if Customer does not renew its applicable Subscription Period on or before the renewal date, Customer will no longer have access to the Rubrik Service, except as set out herein. Upon expiration or termination, Customer will uninstall any Rubrik software components and destroy the Documentation. For a period of thirty (30) days after such termination or expiration, upon Customer's prior written request, Rubrik will allow Customer limited access to retrieve any Customer Data remaining on the Rubrik Service, subject to Customer's compliance with the AUP. After such thirty (30) day grace period, Customer will have no further rights or access to the Rubrik Service, and Customer's Rubrik Service instance, including any Customer Data, will be permanently deleted by Rubrik. The terms of this Agreement shall remain in full force and effect for the period of any post-termination access to the Rubrik Service by Customer.

14.3 Surviving Provisions. Upon expiration or termination of this Agreement, the following sections will survive: Sections 1 (Definitions), 4 (Proprietary Rights), 5 (Orders; Fees), 6 (Verification), 7.2 (Restrictions), 8 (Confidentiality), 11.3 (Disclaimer of

Warranties), 12 (Indemnification), 13 (Limitation of Liability), 14.2 (Post-Termination Obligations)

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L16 – Service Category 16: Enterprise Security Log Management, Analytics, and Response

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Palo Alto Networks Cortex XSIAM

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.

- Names. Respondents must provide their name and the proposed Solution name in the spaces above.

- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.

- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Enterprise Security Log Management, Analytics, and Response consists of multiple components that support and provide enterprise security operations, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and backend capabilities for log collection, storage, aggregation and analytics. This service category enables organizations to monitor, detect, and respond to security threats and provide operational visibility across their technology infrastructure.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM provides an integrated solution for enterprise security operations by combining SIEM, SOAR, and backend capabilities for log collection, storage, aggregation, and analytics. This unified service enables organizations to continuously monitor, detect, and respond to security threats while offering real-time operational visibility across the entire technology infrastructure. By centralizing log management and automating threat detection and response, XSIAM improves efficiency, accelerates incident resolution, and enhances overall security posture.

XSIAM includes SOAR capabilities focused on automating security operations workflows to enhance efficiency and reduce manual intervention. This component streamlines the process of investigating, responding to, and remediating security incidents. XSIAM includes pre-built and customizable playbooks for automating response workflows. It also orchestrates actions across a wide range of security tools and systems to ensure a coordinated and rapid response.

XSIAM's log management capabilities enable secure collection, aggregation, storage, and retrieval of log data, all while ensuring compliance with industry regulations. The platform's backend infrastructure ensures that logs are stored and managed efficiently, and can be easily queried for future analysis. XSIAM is designed to handle large volumes of log data, supporting scalability, enabling organizations to store logs from millions of devices and systems over long periods without compromising performance. Logs from different sources (network, endpoints, servers, cloud platforms, etc.) are aggregated into a central repository, making it easier to search and correlate data for investigations.

XSIAM integrates advanced analytics to detect security threats, identify patterns, and drive automated responses. The platform uses both traditional rule-based approaches and AI-powered models to detect a broad range of threats. XSIAM leverages machine learning to build baselines of normal user and network behavior. When deviations from these baselines are detected (e.g., unusual login times or sudden spikes in data transfer), the platform can generate alerts and trigger responses. XSIAM also analyzes security events and user activities over time to identify anomalous behavior, such as lateral movement, privilege escalation, or data exfiltration.

In conclusion, Cortex XSIAM is a comprehensive platform that provides the full capabilities of a next generation Security Operations Center. By combining real-time data collection, advanced analytics, automated workflows, and threat intelligence, XSIAM empowers security teams to proactively detect and respond to threats, while also offering deep operational visibility to improve security posture.

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Administrator-Guide

https://www.paloaltonetworks.com/resources/techbriefs/cortex-xsiam

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Data Collection and Aggregation – Solution should gather log data from multiple sources, including endpoints, servers, and applications, centralizing them for analysis. It supports structured and unstructured log formats like Syslog and JSON and provides or integrates with cybersecurity analysis solutions (such as SIEM).

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM acts as a data collection and aggregation point, ingesting data, analyzing it for important events and alerts, and initiating automated actions. As a complete SOC tool, XSIAM gathers data from the entire enterprise, prioritizes what is important, and displays it in comprehensive dashboards for improved visualization. Similarly, Cortex XSOAR complements and supplements SIEM tools by orchestrating automated responses across the enterprise.

Prompt 3: Long-Term Data Storage – Solution should provide scalable storage solutions like data and security lakes and archiving to ensure long-term retention of logs for compliance purposes. This includes cloud and on-premises storage with secure, tamper-proof archiving. Options including long-term/cold storage should be available.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Palo Alto Networks offers flexible, scalable storage options that include customizable retention periods. When leveraging our cloud storage offerings, Florida Agencies can choose between hot and cold storage options that suit their SLA requirements and cost preferences. On-premise storage configurations are also available and we work with a variety of options including local databases, file storage solutions, as well as 3rd party integrations like Elastic.

Prompt 4: Security Event Correlation - Solution should provide real-time event correlation, detecting complex attacks and anomalies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSIAM addresses real-time event correlation with advanced analytics engine. It continuously ingests and normalizes data from diverse sources, using ML models to detect complex attack patterns and anomalies. Correlating events across the network, endpoints, and cloud environments, XSIAM identifies sophisticated threats. Our automated playbooks and detailed dashboards provide actionable insights, enabling rapid response and threat mitigation.

Prompt 5: Big Data Engine – Solution should process and analyze large volumes of security data in real time. By leveraging distributed computing frameworks this component enables complex threat detection, pattern recognition, and predictive analytics across large data sets. Provide training data sets to reduce false alerts and optimize efficiency of the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSIAM processes & analyzes large volumes of security data in real time with scalability and flexibility of SaaS solutions. Using distributed computing frameworks enables complex threat detection, pattern recognition, and predictive analytics. Ingesting diverse data sources, applies AI/ML models to correlate events, and generates actionable insights. It's continuous learning reduces false alerts and optimizes efficiency, providing real time security event correlation.

Prompt 6: Microservices Architecture – Solution should provide a modular approach to security operations, allowing individual services (e.g., log collection, incident response, threat detection) to operate independently. This architecture ensures scalability and flexibility, allowing organizations to adapt to evolving security needs without overhauling the entire system.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

The entire Cortex platform has a microservice architecture. Both are extensible with REST APIs supporting modularity and interoperability with a wide vendor ecosystem. The Cortex marketplace supports over 1,000 third-party integrations with major industry partners. This allows each Florida agency to quickly incorporate preferred technologies into a comprehensive system that adapts to changing needs without a complete overhaul.

Prompt 7: Monitoring and Threat Detection – Solution should provide continuous real-time monitoring with customizable alerts and advanced analytics that identify threats using machine learning, AI, and behavioral analysis. Integration with threat intelligence ensures proactive threat detection and enriched security alerts with additional threat intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM continuously collects data from a wide array of security systems, devices, and services to ensure comprehensive real-time monitoring and threat detection to provide visibility across the entire network. XSIAM combines traditional signature-based detection with behavioral analytics, machine learning, and AI-driven models to identify and flag malicious activity. XSIAMs baselines normal system behavior and uses advanced analytics to detect anomalous actions.

Prompt 8: Log Management. Solution should provide centralized or federated management of logs, enabling real-time indexing and analysis of security events. It ensures that logs are stored and managed according to compliance standards, with flexible retention policies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

XSIAM centralizes log data from a wide range of sources, including, security tools, network devices, cloud services, SIEMs, applications, operating systems, and other system logs. By aggregating logs from these disparate sources, XSIAM enables security teams to have a unified view of their security environment and ensures they can correlate events across different systems for more effective detection and response.

Prompt 9: Incident Response and Automation - Solution should automate responses, isolating compromised systems or blocking malicious activity based on predefined playbooks. Incident management tools provide a centralized view of security events from detection to resolution.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSIAM automates incident response through the use of playbook-driven workflows. These workflows orchestrate tasks across multiple systems through the use of event-driven triggers. For example, if a malicious activity is detected on an endpoint, XSIAM can execute an automated playbook response that can disable network access, notify security administrators, open an incident response ticket, and take other actions.

Prompt 10: Case Management and Collaboration – Solution should track incidents through case management, documenting all actions taken for compliance. Collaboration tools ensure effective communication among security team members.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Cortex XSOAR (a component of XSIAM) provides case management and collaboration capabilities for managing critical security incidents, improving response times, and enhancing teamwork during investigations. These features streamline security operations by organizing, automating, and enabling seamless communication between teams, which helps Agencies to efficiently track and manage incidents across the full lifecycle, from detection to resolution.

Prompt 11: Analytics and Reporting – Solution should provide powerful tools for transforming raw security data into meaningful insights. Customizable dashboards and reports help security teams and decision-makers visualize security metrics, alerts, and trends in real time. End User integration allows the platform to connect with business intelligence (BI) tools for further analysis and reporting.

Please describe if and how Respondent’s proposed Solution meets the above prompt in the field below.

Cortex XSIAM's customizable dashboards visualize data, monitor security operations, and provide real-time insights into incidents, alerts, and security metrics. Florida agencies can tailor dashboards to display critical metrics, including time-based alerts, top threat indicators, MTTR, and MTTD. XSIAM also integrates with BI tools like Tableau via Cortex marketplace.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Cortex Products

Service-Level Agreement

All capitalized terms not defined herein shall have the same meaning as set forth in the Palo Alto Networks End User Agreement.

Cortex XSIAM, XDR, XSOAR, and Xpanse-hosted services shall be available 99.9% of the time, measured monthly, excluding scheduled maintenance. Further, any downtime resulting from outages of third-party connections or utilities or other reasons beyond the control of Palo Alto Networks will be excluded.

Customer’s sole and exclusive remedy and the entire liability of Palo Alto Networks, in connection with Cortex product service availability, shall be to credit customer 2% of monthly service fees (downtime credit) for each breach. A breach is defined as a period of 60 consecutive minutes of downtime (delays in data log ingestion are not considered downtime). Downtime shall begin to accrue as soon as customer notifies Palo Alto Networks that the service is down and will continue to accrue until service is restored.

In order to receive downtime credit, customers must notify Palo Alto Networks within 24 hours of service unavailability by initiating a help desk ticket. Failure to provide such notice forfeits the right to receive downtime credit. Such credits may not be redeemed for cash and shall not exceed one (1) week of service fees in any one (1) calendar month. Blocking of data communications or other software as a service (SaaS) by Palo Alto Networks in accordance with its Information Security policies shall not constitute a failure to provide adequate service under this Service-Level Agreement.

Palo Alto Networks will provide technical support based on the Customer Success Plan purchased:

- Under the Standard Plan, technical support is available via the Customer Support Portal.
- Under the Premium Plan, technical support is also available as above and by phone 24 hours per day, 7 days per week.

Customers may initiate a help desk ticket via support.paloaltonetworks.com. Palo Alto Networks will use commercially reasonable efforts to respond as follows:

Severity Level 1: Service is down; critically affects customer production environment. No workaround available yet. Standard: less than/equal to 2 hours; Premium: less than/equal to 1 hour

Severity Level 2: Service is impaired; customer production up, but impacted. No workaround available yet. Standard: less than/equal to 4 hours; Premium: less than/equal to 2 hours

Severity Level 3: A service function has failed; customer production not affected Support is aware of the issue and a workaround is available. Standard: less than/equal to 12 hours; Premium: less than/equal to 4 hours

Severity Level 4: Non-critical issue. Does not impact customer business. Feature, information, documentation, how-to, and enhancement requests from customer. Standard: less than/equal to 48 hours; Premium: less than/equal to 8 business hours

More Information

To learn more about Palo Alto Networks Support offerings, visit paloaltonetworks.com/support or contact your local account manager. For product information, visit paloaltonetworks.com/products.

Why Palo Alto Networks?

Palo Alto Networks is committed to your success in preventing successful cyberattacks. Our award-winning services and support organization give you timely access to technical experts and on- line resources to ensure your business is protected. We take our responsibility for your success seriously and continuously strive to deliver an exceptional customer experience. Our entire services organization and Authorized Support Centers are there to ensure maximum uptime and streamlined operations.

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT (“Agreement”) GOVERNS THE USE OF PALO ALTO NETWORKS PRODUCTS

(as that term “Product” is defined below).

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND

(A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054, UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; (B) PALO ALTO NETWORKS (UK) LTD, 22 BISHOPSGATE, LEVEL 55 , LONDON, EC2N 4BQ, ENGLAND. IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA; OR (C) PALO ALTO NETWORKS PUBLIC SECTOR LLC, IF YOU ARE A UNITED STATES FEDERAL GOVERNMENT ENTITY OR ORGANIZATION (EACH OF THE ENTITIES LISTED IN (A), (B) OR (C) BEING REFERRED TO HEREIN AS “PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS AGREEMENT GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION IF ACQUIRED THROUGH PALO ALTO NETWORKS OR AN AUTHORIZED AFFILIATE OF PALO ALTO NETWORKS, OR AN

AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR CLOUD MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER

SUPPORT AGREEMENT FOUND AT www.paloaltonetworks.com/legal/eusa WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS AGREEMENT.

If you use a Product for proof of concept, trial, evaluation or other similar purpose (“Evaluations”), you may do so for 30 days only unless Palo Alto Networks issues an extension. Palo Alto Networks reserves the right to terminate Evaluations at any time. Upon expiration or termination of the Evaluation, you shall cease using the Product(s) provided for Evaluation and must return any Evaluation Hardware to Palo Alto Networks in the same condition as when first received, except for reasonable wear and tear. For Evaluations and products provided pursuant to a Product Donation Agreement, only sections 1, 2, 3, 7, 9, 10, and 11 of this Agreement shall apply, as well as section 6 for products provided pursuant to a Product Donation Agreement, and PALO ALTO NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY AGAINST INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

1. DEFINITIONS

“Affiliate” means any entity that Controls, is Controlled by, or is under common Control with Customer or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

Customer acknowledges and authorizes Palo Alto Networks’ use of all Palo Alto Networks Affiliates to deliver Products and Services.

“End User Data” means data that is provided by or on behalf of You to Palo Alto Networks during the relationship governed by this Agreement. For the avoidance of doubt, End User Data does not include Systems Data.

“Enterprise Program” means a volume usage arrangement, valid for a specified term, during which End User may access certain Software, Subscriptions, and/or related technical support.

“Hardware” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“Product” means, collectively, Hardware, Software, Subscription, or any combination thereof, regardless of whether or not the Product was procured under an Enterprise Program.

“Published Specifications” mean the applicable user manual, the WildFire Acceptable Use Policy found at https://www.paloaltonetworks.com/resources/datasheets/wildfire-acceptable-use-policy, the applicable Service Level Agreement found at https://www.paloaltonetworks.com/services/support/support-policies.html , and other corresponding materials published by Palo Alto Networks that are customarily made available to End Users of the applicable Product. “Software” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

"Subscription(s)" means Software-as-a-Service and cloud-delivered security services, including updates, provided by Palo Alto Networks including, but not limited to, Cortex, Prisma, Advanced Threat Prevention, Advanced URL Filtering, Advanced WildFire, regardless of whether a fee is charged for its use. Technical support, customer success plans, and professional services are not considered Subscriptions under this Agreement.

"Systems Data" means data generated or collected in connection with Your use of the Products, such as logs, session data, telemetry data, support data, usage data, threat intelligence or actor data, statistics, netflow data, potentially malicious files detected by the Product, and derivatives thereof.

2. USE AND RESTRICTIONS

a. Software Use Rights

This section 2a applies to Software only. Subject to your compliance with this Agreement, Palo Alto Networks grants you a limited, royalty-free, non-exclusive right to use the Software:

i. in accordance with Published Specifications for the Product;

ii. solely within the scope of the use rights purchased (e.g., number of users);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights in the Software are expressly reserved by Palo Alto Networks.

b. Access to Subscriptions

This section 2b applies to Subscriptions only. During the term of the Subscriptions purchased and subject to your continuous compliance with this Agreement, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 11g below. Palo Alto Networks grants you a non-exclusive right to access and use the Subscriptions:

i. in accordance with Published Specifications for the Product;

ii. solely within the usage capacity purchased (e.g., number of workloads);

iii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and

iv. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this Agreement.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions You shall not:

i. use any Product that is procured under a Lab or NFR (not for resale) SKU in a production environment;

ii. use the Products beyond the scope of the use right and/or capacity purchased;

iii. modify, translate, adapt or create derivative works from the Products, in whole or in part;

iv. disassemble, decompile, reverse engineer or otherwise attempt to derive or create derivative works of the source code, methodology, analysis, or results of the Products, in whole or in part, unless expressly permitted by and only to the extent of applicable law in the jurisdiction of use despite this prohibition;

v. remove, modify, or conceal any product identification, copyright, proprietary or intellectual property notices or other such marks on or within the Product;

vi. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;

vii. Transfer, sublicense, or assign your rights under this Agreement to any other person or entity except as expressly provided in section 2d below, unless expressly authorized by Palo Alto Networks in writing;

viii. sell, resell, sublicense, rent, lease, loan, assign, or otherwise transfer the Products or any rights or interests in the Products to any third party except in accordance with the express terms herein. Products purchased from unauthorized resellers or other unauthorized entities shall be subject to the Palo Alto Networks license transfer procedure (https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html);

ix. use Software that is licensed for a specific device, whether physical or virtual, on another device, unless expressly authorized by Palo Alto Networks in writing;

x. duplicate or copy the Software, its methodology, analysis, or results unless specifically permitted in accordance with Published Specifications for such Software, or for the specific purpose of making a reasonable number of archival or backup copies, and provided in each case that you reproduce in the copies the copyright and other proprietary notices or markings that appear on the original copy of the Software as delivered to you;

xi. use the Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or intellectual property rights;

xii. use the Subscriptions in any manner not authorized by the Published Specifications for the Product;

xiii. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein; or

xiv. provide access to or otherwise make the Products or the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, managed services provider, service bureau or other type of service unless specifically permitted by the Published Specifications or agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

i. provide the Affiliate with a copy of this Agreement;

ii. ensure that the Affiliate complies with this Agreement;

iii. be responsible and liable for any breach of this Agreement by such Affiliate; and

iv. where applicable, be responsible and liable for any local law that imposes any tariffs, fees, penalties, or fines arising from your Affiliates' use of the Product in such jurisdictions.

e. Authentication Credentials

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any misuse of your accounts or authentication credentials.

3. OWNERSHIP

Palo Alto Networks and its licensors/suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, database rights, trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. Your rights to use the Product are limited to those expressly granted in this Agreement. All rights not expressly granted are retained by Palo Alto Networks and/or its licensors/suppliers. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

4. OVERUSE.

Fees which are payable in advance for volume or capacity usage Subscriptions (e.g., number of accounts, credits, endpoints, devices, points, seats, terabytes of data, tokens, users, workloads, etc.) must be reconciled with your actual usage at the end of each month or quarter for any volume or capacity-based Subscriptions. Palo Alto Networks (or, where applicable, the relevant Palo Alto Networks Affiliate) reserves the right to perform true-up reconciliation and charge (via the applicable Palo Alto Networks Affiliate or your authorized reseller or cloud marketplace) for any such usage above the volume or capacity purchased. Unless agreed otherwise in writing, this calculation will be based on the Palo Alto Networks' then current price list. You will issue a non-cancellable, non-refundable and non-returnable purchase order for such overuse within ten (10) days from the occurrence of such overuse and pay as invoiced. If payment is not received in a timely fashion for such overuse, Palo Alto Networks shall terminate or suspend your use of such Subscriptions in accordance with Section

5. b., below.

5. TERM; TERMINATION OR SUSPENSION; AND EFFECT OF TERMINATION

a. Term.

This Agreement is effective for the duration of the order (specifically for the Software, Subscription or Support Service term) to which this Agreement relates, subject to earlier termination according to this Agreement, including without limitation any extension of such order involving a purchase that increases the quantity initially ordered (e.g. additional capacity).

b. Termination; Suspension

i. Palo Alto Networks may terminate this Agreement at any time in the event you breach any material term, including but not limited to exceeding the use or capacity restrictions (Section 2 above) as purchased or as stated in applicable Published Specifications, and fail to cure such breach within thirty (30) days following notice.

ii. Palo Alto Networks may, at its discretion, terminate or suspend your access to or use of Software or Subscriptions or Support Services if you are in default with any payment obligations concerning the Product or Support Services due to Palo Alto Networks, a cloud service provider marketplace, an authorized reseller, or to any third-party finance company that financed the purchase of the Product on your behalf.

iii. In addition to the termination rights set forth above, Palo Alto Networks reserves the right to suspend Customer's access to or use of Software or Subscriptions or Support Services if Palo Alto Networks reasonably believes that Customer is using the services in manner or for a purpose that is likely to cause harm to Palo Alto Networks or a third party.

c. Effects of Termination

Upon termination, you shall immediately cease using the Product and in case of Software and/or Subscriptions, Palo Alto Networks shall terminate your use of or access to any Subscriptions and access to Support Services. At Palo Alto Network´s discretion, you shall destroy or return to Palo Alto Networks all copies of Palo Alto Networks' Confidential Information.

6. WARRANTY, EXCLUSIONS AND DISCLAIMERS

a. Warranty

Palo Alto Networks warrants that:

i. Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;

ii. Software shall substantially conform to Palo Alto Networks' Published Specifications for three (3) months from the date of fulfillment; and

iii. Subscriptions shall perform materially to Published Specifications for the duration of the selected term.

As your sole and exclusive remedy and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of this warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made within ten (10) days from the detection of a suspected defect /discrepancy in writing during the warranty period specified herein, if any. If after using commercially reasonable efforts, Palo Alto Networks, determines in its sole discretion, that it is unable to repay or replace the Product, Customer will be entitled to a refund of the fees paid by the Customer for that portion of the Product that did not comply with the warranty.

Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

b. Exclusions

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or its designee;

ii. accident, negligence, abuse or misuse of a Product;

iii. use of the Product other than in accordance with Published Specifications;

iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the Published Specifications including, without limitation, temperature or humidity ranges; or

v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

c. Disclaimers

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS, ITS LICENSORS, AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (I) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (II) THE USE OF PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE, OR (III) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

7. LIMITATION OF LIABILITY

a. Disclaimer of Indirect Damages

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of business, goodwill, data, profits, or use or for the cost of procuring substitute products, services or other goods), arising out of or relating to the Products to which this Agreement relates, regardless of the theory of liability and whether or not each party was advised of the possibility of such damage or loss.

b. Direct Damages

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to the Products to which this Agreement relates, exceed the greater of one million United States dollars or the total amount you paid for the entire term of the Subscription or Enterprise Program on which the claim is based. The foregoing limitation in this section 8b shall not apply to liability arising from:

i. death or bodily injury;

ii. sections 2 (Use and Restrictions) and 8 (Indemnification); and

iii. Customer's payment obligations for the Product and related services, if any.

8. INDEMNIFICATION

a. Indemnification and Procedure

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that a Product infringes or misappropriates such third party's patent, copyright, trademark, database right, trade secret or other intellectual or intangible property right (a "Claim"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks to the extent attributable to any such Claim; provided that you (i) promptly notify Palo Alto Networks in writing of the Claim; (ii) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (iii) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

b. Remedy

If a Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

i. procure the right for you to continue using the Product;

ii. replace or modify the Product to avoid the Claim; or

iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section 8 shall not apply to the extent any Claim results from or is based on:

i. modifications to a Product made by a party other than Palo Alto Networks or its designee;

ii. the combination, operation, or use of a Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;

iii. failure to use (1) the most recent version or release of a Product, or (2) an equally compatible and functionally equivalent, non-infringing version of a Product supplied by Palo Alto Networks to address such Claim;

iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or

v. use of a Product not in accordance with Published Specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL AND INTANGIBLE PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

9. CONFIDENTIALITY

"Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of initial disclosure by the disclosing party ("Discloser"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("Recipient"). Confidential Information does not include Systems Data. Confidential Information also does not include information that Recipient can prove by credible evidence:

i. was in the public domain at the time it was communicated to Recipient;

ii. entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;

iii. was in Recipient's possession free of any obligation of confidentiality at the time it was communicated to Recipient;

iv. was disclosed to Recipient free of any obligation of confidentiality; or

v. was developed by Recipient without use of or reference to Discloser's Confidential Information.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this Agreement, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors who need to know such Confidential Information for the performance of this Agreement, provided that each such employee and subcontractor is subject to use and disclosure restrictions that are at least as protective as those set forth herein. Recipient shall maintain the confidentiality of Discloser's Confidential Information using the same effort that it ordinarily uses with respect to its own confidential information of similar nature and importance, but no less than reasonable care. The foregoing obligations will not restrict Recipient from disclosing Discloser's Confidential Information:

a. pursuant to an order issued by a court, administrative agency, or other governmental body, provided that the Recipient gives reasonable notice to Discloser to enable it to contest such order;

b. on a confidential basis to its legal or professional financial advisors; or

c. as required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this Agreement, whichever is later.

10. END USER DATA AND SYSTEMS DATA

a. End User Data

Palo Alto Networks and its Affiliates will process End User Data solely for the purposes of fulfilling its obligations under the terms of this Agreement. To the extent Palo Alto Networks and its Affiliates processes personal data, as defined by applicable data protection laws, such personal data will be processed in accordance with the Data Processing Addendum, which is incorporated by reference herein.

b. Systems Data

Palo Alto Networks may use Systems Data to provide Products and services to You, to improve Products and services, to develop new Products and services, to manage our relationship with You, and for threat research purposes. Palo Alto Networks will not disclose to any unaffiliated third-party Systems Data that identifies You, Your customers or end users, except to the extent required to comply with applicable law or valid order of a court or government agency of competent jurisdiction.

11. GENERAL

a. Assignment

Neither party may assign or transfer this Agreement or any obligation herein without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this Agreement or any obligation herein to its Affiliate, or an entity acquiring all or substantially all assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this Agreement (except as permitted under the terms herein) shall be null and of no effect. For purposes of this Agreement, a change of Control will be deemed to be an assignment. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You shall retain records pertaining to Product usage. You grant to Palo Alto Networks and its independent advisors the right to examine such records no more than once in any twelve-month period solely to verify compliance with this Agreement. In the event such audit reveals non-compliance with this Agreement, you shall promptly pay the appropriate fees, plus reasonable audit costs, as determined by Palo Alto Networks.

c. Authorization Codes; Grace Periods

Where applicable, you will be able to download Software via the server network located closest to you. Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the

time of order fulfillment. The Subscription, warranty or support term will commence in accordance with the grace period policy at https://www.paloaltonetworks.com/support/support-policies/grace-period.html

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your activities arising from this Agreement. You further agree that you will not engage in any illegal activity, and you acknowledge that Palo Alto Networks reserves the right to notify you or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations where applicable, and any other applicable export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this Agreement or otherwise.

f. Entire Agreement

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understanding and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with, in addition to, or purport to vary the terms and conditions of this Agreement are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption, or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, epidemic or pandemic, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott, availability of network and telecommunications services or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the state or federal courts located in Santa Clara County, California. If you are located outside North or Latin America, this Agreement shall be governed by and construed in accordance with the laws of England and Wales, excluding its conflict of laws principles. Any legal action or proceeding arising under this Agreement will be brought exclusively in the courts of London, England. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered:

i. for Customer, to the e-mail set forth on the Customer's website and to an officer of Customer, or as otherwise provided by Customer to Palo Alto Networks for the purpose of effectuating written notices.

ii. for Palo Alto Networks: legal@paloaltonetworks; or,

iii. for either party, by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open-Source Software

The Products may contain or be provided with components subject to the terms and conditions of open-source software licenses ("Open-Source Software"). A list of Open-Source Software can be found at https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html. These Open-Source Software license terms are consistent with the rights granted in section 2 (Use and Restrictions) and may contain additional rights benefiting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this Agreement, does not include Open-Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "QATT") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all

claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Marketing

Customer hereby grants to Palo Alto Networks the right to use Customer's name, logo and related marks in marketing and sales materials and communications

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L16 – Service Category 16: Enterprise Security Log Management, Analytics, and Response

Respondent Name: Blackwood Associates, Inc. (Blackwood)

Solution Name: Splunk SIEM

Respondent Instructions:

- Respondents shall use this Attachment as provided to respond. Altering character count limits or any other restriction or control may result in a Respondent being found non-responsive.
- Names. Respondents must provide their name and the proposed Solution name in the spaces above.
- Section 1 Prompts. Section 1 of this attachment provides prompts. The Respondent shall provide a response to prompt 1 and should provide responses to prompts 2 through 11. Prompts are indicated by red text followed by a response block.

  Prompt 1 has a maximum of 3000 characters. Prompts 2 through 11 have a maximum character limit of 500. Respondents who submit responses outside of the maximum character limit may be deemed non-responsive. Any additional files, links, or other information provided outside the response block will not be considered for evaluation.

  Scores will be assigned by each individual evaluator in accordance with Attachment C, Evaluation Criteria. Prompt 1 is worth a total of 5 points. Prompts 2 through 11 are worth a maximum of 4 points total. An individual Evaluator's score of the technical response for a proposed Solution will be calculated by the following:

  > Evaluator's Prompt 1 score + (Sum of the Evaluator's Scores for Prompts 2-11 / 10) = Evaluator's Technical Response Score

- Section 2 Terms and Conditions. Section 2 of this attachment provides a space for the Respondent to include any Service Level Agreements (SLA) or additional terms and conditions that apply to the proposed Solution. Neither the SLAs nor the additional terms and conditions will be considered for evaluation.
- Definitions. Definitions contained in Attachment A, Statement of Work, are incorporated by reference.

Section 1. Prompts.

Prompt 1: Enterprise Security Log Management, Analytics, and Response consists of multiple components that support and provide enterprise security operations, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and backend capabilities for log collection, storage, aggregation and analytics. This service category enables organizations to monitor, detect, and respond to security threats and provide operational visibility across their technology infrastructure.

Please describe how Respondent's proposed Solution meets the above prompt in the field below.

Splunk's Enterprise Security solution is designed to meet and exceed the requirements of Service Category 16 by offering a comprehensive suite of capabilities that address security log management, analytics, and response. By combining SIEM, SOAR, and extensive log management, Splunk delivers a powerful, integrated solution that strengthens the State of Florida's ability to monitor, detect, and respond to threats.

Splunk's SIEM capabilities centralize and normalize log data from a variety of sources, including network devices, endpoints, cloud services, and applications, enabling real-time monitoring and alerting. By using advanced data correlation and analytics, Splunk identifies and prioritizes potential threats, allowing security teams to quickly detect, investigate, and mitigate incidents. The solution is flexible and customizable, with configurable detection rules, dashboards, and reporting to align with specific compliance needs and security policies.

The Splunk platform is designed for high-volume log collection and aggregation, with scalable storage options that can accommodate the vast data requirements of an enterprise environment. The solution provides seamless data ingestion, indexing, and search capabilities, enabling rapid access to critical logs for analysis and auditing. Splunk supports both on-premises and cloud storage solutions, providing flexibility to align with the State's retention policies and compliance requirements.

Splunk incorporates advanced analytics and machine learning to enhance threat detection accuracy and operational efficiency. By leveraging behavioral analysis and anomaly detection, Splunk can proactively detect unknown threats and prioritize them based on risk. Machine learning algorithms continuously learn from historical data to improve threat detection and reduce false positives, enabling the State's security team to focus on high-priority threats and optimize resource allocation.

Splunk's SOAR capabilities support the automation of incident response workflows, accelerating response times and improving consistency. The platform offers customizable playbooks that automate key actions, such as threat containment, isolation, and remediation, based on defined conditions. This automation reduces manual intervention, minimizes response time, and ensures that incidents are handled efficiently. Splunk's SOAR integrates seamlessly with existing tools, enabling streamlined orchestration across the security stack.

Splunk provides real-time visibility into the entire IT ecosystem through customizable dashboards and in-depth reporting, allowing the State of Florida to monitor key performance indicators (KPIs) and security metrics continuously. This enhanced visibility supports regulatory compliance, with comprehensive audit logs, pre-configured reporting templates, and customizable reports to meet specific regulatory standards.

For the prompts below (indicated by red text followed by a response block), the Respondent should provide details on if and how the Solution meets the identified technical capabilities and features.

Prompt 2: Data Collection and Aggregation – Solution should gather log data from multiple sources, including endpoints, servers, and applications, centralizing them for analysis. It supports structured and unstructured log formats like Syslog and JSON and provides or integrates with cybersecurity analysis solutions (such as SIEM).

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk Enterprise and Enterprise Security collect data from diverse sources, including endpoints, servers, and applications. It supports both structured and unstructured log formats (e.g., Syslog, JSON) and centralizes logs for analysis. Splunk ES is a comprehensive SIEM solution that integrates with other cybersecurity tools, enabling advanced insights and streamlined incident response to meet security and compliance needs.

Prompt 3: Long-Term Data Storage – Solution should provide scalable storage solutions like data and security lakes and archiving to ensure long-term retention of logs for compliance purposes. This includes cloud and on-premises storage with secure, tamper-proof archiving. Options including long-term/cold storage should be available.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk provides scalable, secure long-term data storage with options across cloud, on-premises, and hybrid setups. Splunk integrates with industry leading data lakes including but not limited to Snowflake, Amazon Security Lake, and other object based storage solutions. Splunk has both hot/active searchable storage, along with archived storage options, to meet regulatory compliance. Splunk offers tamper-proofing with auto-archiving capabilities.

Prompt 4: Security Event Correlation - Solution should provide real-time event correlation, detecting complex attacks and anomalies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk's SIEM platform delivers real-time event correlation, identifying complex attack patterns and anomalies by analyzing data across multiple sources. Its advanced analytics detects complex attacks, anomalies, and suspicious behaviors and correlate events to provide context, enabling rapid threat detection and response. This capability allows security teams to efficiently uncover hidden threats and act on security incidents proactively, enhancing the overall posture

Prompt 5: Big Data Engine – Solution should process and analyze large volumes of security data in real time. By leveraging distributed computing frameworks this component enables complex threat detection, pattern recognition, and predictive analytics across large data sets. Provide training data sets to reduce false alerts and optimize efficiency of the platform.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk's platform efficiently processes and analyzes massive data volumes in real-time, using a highly scalable, distributed architecture. Splunk indexes data for rapid retrieval, enabling advanced analytics. With AI/ML integration, Splunk supports predictive insights and anomaly detection, helping customers gain valuable, actionable intelligence from big data at scale. Splunk provides training datasets that allow machine learning models to learn from historical data.

Prompt 6: Microservices Architecture – Solution should provide a modular approach to security operations, allowing individual services (e.g., log collection, incident response, threat detection) to operate independently. This architecture ensures scalability and flexibility, allowing organizations to adapt to evolving security needs without overhauling the entire system.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk supports microservices architecture by enabling real-time monitoring and visibility into containerized applications across distributed environments. It collects and correlates logs, metrics, and traces from microservices, providing a unified view for troubleshooting and performance optimization. With integrations for Kubernetes and Docker, Splunk aids in managing complex, dynamic microservices, ensuring reliability, scalability, and faster issue resolution.

Prompt 7: Monitoring and Threat Detection – Solution should provide continuous real-time monitoring with customizable alerts and advanced analytics that identify threats using machine learning, AI, and behavioral analysis. Integration with threat intelligence ensures proactive threat detection and enriched security alerts with additional threat intelligence.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk provides continuous real-time monitoring with customizable alerts and advanced analytics powered by AI/ML, and behavioral analysis, enhanced by Risk-Based Alerting (RBA). RBA prioritizes threats based on risk scores, reducing alert fatigue and enabling faster, targeted responses. Integrated threat intelligence ensures proactive detection and enriched alerts, with adaptive response capabilities to automate responses and strengthen overall security posture.

Prompt 8: Log Management. Solution should provide centralized or federated management of logs, enabling real-time indexing and analysis of security events. It ensures that logs are stored and managed according to compliance standards, with flexible retention policies.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk offers centralized and federated multi-site log management, providing real-time indexing and analysis across locations. Splunk supports flexible retention policies to meet compliance standards and ensures log integrity through encryption, hashing, and audit trails. With encryption at rest and encryption in transit, Splunk securely stores logs in cost-effective, scalable tiers, ensuring long-term data accessibility and compliance adherence across environments.

Prompt 9: Incident Response and Automation - Solution should automate responses, isolating compromised systems or blocking malicious activity based on predefined playbooks. Incident management tools provide a centralized view of security events from detection to resolution.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk enables automated incident response through predefined playbooks. Splunk ES correlates security events in real-time, while SOAR automates workflows to isolate compromised systems or block malicious activity. The solution provides a centralized view of security events, while automating repetitive tasks, ensuring efficient management from detection to resolution, improving response times and minimizing manual intervention.

Prompt 10: Case Management and Collaboration – Solution should track incidents through case management, documenting all actions taken for compliance. Collaboration tools ensure effective communication among security team members.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk supports case management and collaboration with a centralized platform for tracking, investigating, and resolving incidents. It integrates with ticketing and collaboration tools to streamline workflows, allowing teams to work efficiently. Users can create cases, share findings, and document actions, ensuring seamless collaboration. Customizable dashboards and real-time data provide stakeholders with relevant information for timely decision-making.

Prompt 11: Analytics and Reporting – Solution should provide powerful tools for transforming raw security data into meaningful insights. Customizable dashboards and reports help security teams and decision-makers visualize security metrics, alerts, and trends in real time. End User integration allows the platform to connect with business intelligence (BI) tools for further analysis and reporting.

Please describe if and how Respondent's proposed Solution meets the above prompt in the field below.

Splunk offers analytics and reporting capabilities, transforming raw security data into actionable insights. Customizable dashboards and reports allow security teams to visualize real-time metrics, alerts, and trends, enhancing situational awareness. With end-user integration support, Splunk connects seamlessly with (BI) tools, enabling deeper analysis and extended reporting to align security insights with broader business objectives for informed decision-making.

Section 2. Service Level Agreement or Additional Terms and Conditions.

Respondent shall include any Service Level Agreements (SLAs) or additional terms and conditions that apply to the proposed Solution in the following text boxes. The text boxes below have a maximum character limit of 32,672 characters each. The information provided in the text boxes below will not be scored but will be incorporated into the final Term Contract documents as an exhibit.

Service Level Commitment

The Splunk Cloud Services will be available 100% of the time, as measured by Splunk over each calendar quarter of the Subscription Term, and subject to the exclusions set forth below (the "Service Level Commitment").

A Splunk Cloud Service is considered available if the Customer is able to login to its Splunk Cloud Service account and initiate a search using Splunk Software.

Service Level Credit:

If Splunk fails to achieve the above Service Level Commitment for a Splunk Cloud Service, Customer may claim a credit for such Splunk Cloud Service as provided below, up to a maximum credit per calendar quarter equal to one month's Splunk Cloud Service subscription fees.

PERCENTAGE AVAILABILITY PER CALENDAR QUARTER	CREDIT
100	NO CREDIT
99.99-99.999	2 HOURS
99.9-99.99	4 HOURS
99.0-99.9	8 HOURS
95.0-99.0	1 DAY
0-95.0	1 MONTH

Exclusions

A Customer will not be entitled to a service credit if it is in breach of its Agreement with Splunk, including payment obligations. The Service Level Commitment does not apply to any downtime, suspension or termination of the applicable Splunk Cloud Service (or any Splunk Content or Splunk Software operating in connection with the Splunk Cloud Service) that results from:

- Account suspension or termination due to Customer's breach of the Agreement.
- Routine scheduled maintenance (Splunk's Maintenance Policy is available at https://www.splunk.com/en_us/legal/splunk-cloud-platform-maintenance-policy.html).
- Unscheduled, emergency maintenance or an emergency caused by factors outside Splunk's reasonable control, including force majeure events such as acts of God, acts of government, flood, fire, earthquake, civil unrest, acts of terror, Customer Content, Third Party Content or Internet Service Provider failures or delays.

- A Customer's equipment, software or other technology, or third-party equipment, software or technology (other than those which are under Splunk's control).

- Failures resulting from software or technology for which Splunk is not responsible under the Agreement.

- Customer's ability or inability to operate the Forwarder software is addressed by Splunk support services. For purposes of the Service Level Commitment, the Forwarder software is excluded from the calculation of the availability of the Splunk Cloud Services.

No Service Level Commitment is provided for free, proof-of-concept or unpaid trial services

Service Credit Claims.

To receive a service credit, a Customer must file a claim for such credit within five (5) days following the end of the calendar quarter in which the Service Level Commitment was not met for an applicable Splunk Cloud Service, by contacting Splunk at splunk-cloud-billing@splunk.com with a complete description of the downtime, how the Customer was adversely affected, and for how long. Splunk reserves the right to deny the service credit if the Customer does not qualify.

The service credit remedy set forth in this Service Level Schedule is the Customer's sole and exclusive remedy for the unavailability of any applicable Splunk Cloud Service.

*All capitalized terms not otherwise defined are as set forth in the Splunk Cloud Terms of Service.

Splunk General Terms > https://www.splunk.com/en_us/legal/splunk-general-terms.html

Last Updated: September 4, 2024

These Splunk General Terms (“General Terms”) between Splunk LLC, a Delaware limited liability company, with its office at 3098 Olsen Drive, San Jose, California 95128, USA (“Splunk” or “we” or “us” or “our”) and you (“Customer” or “you” or “your”) govern your acquisition, access to, and use of Splunk’s Offerings, regardless of how accessed or acquired, whether directly from us or from another Approved Source. By clicking on the appropriate button, or by downloading, installing, accessing, or using any Offering, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to these General Terms, or if you are not authorized to accept the General Terms on behalf of Customer, do not download, install, access, or use any Offering. The “Effective Date” of these General Terms is: (i) the date of Delivery; or (ii) the date you access or use the Offering in any way, whichever is earlier. Capitalized terms are defined in the Definitions section below.

1. Your Use Rights and Limits

- Your Use Rights. We grant you a non-exclusive, worldwide, non-transferable and non-sublicensable right, subject to your compliance with these General Terms and payment of applicable Fees, to use acquired Offerings only for your Internal Business Purpose during the Term, up to the Capacity, and, if applicable, in accordance with the Order (“Use Rights”). You have the right to make a reasonable number of copies of On-Premises Products for archival and back-up purposes.

- Limits on Your Use Rights. Except as expressly permitted in the Order, these General Terms or Documentation, your Use Rights exclude the right to, and you agree not to (nor allow any user or Third Party Provider to): (i) reverse engineer, decompile, disassemble or otherwise attempt to discover source code or underlying structures, ideas, protocols or algorithms of, or used by, any Offering; (ii) modify, translate or create derivative works based on any Offering; (iii) use an Offering to ingest, process, monitor, analyze or service the devices, systems, networks or application data of any third party; (iv) resell, sublicense, rent the use of, transfer or distribute any Offering; (v) access or use an Offering to analyze, test, characterize, inspect, or monitor its availability, performance, or functionality for competitive purposes; (vi) access or use an Offering to develop, test, troubleshoot, support, or market any software or service that competes with any Offering, or that integrates, interoperates with, or constitutes an extension of any Offering and that you use or intend to use for a commercial purpose; (vii) access or use any Offering in order to analyze, test, characterize, inspect, or monitor its source code or underlying structures, ideas, protocols, or algorithms it contains or uses; (viii) attempt to disable or circumvent any license key or other technological mechanisms or measures intended to prevent, limit or control use or copying of, or access to, Offerings; (ix) separately use any of the applicable features and functionalities of the Offerings with external applications or code not furnished by us or any data not processed by the Offering; (x) exceed the Capacity; or (xi) use any Offering in violation of any applicable laws and regulations (including but not limited to any applicable data protection and intellectual property laws). For clarity, each of the foregoing subsections imposes a separate and independent limit on your Use Rights.

- Splunk Extensions. Your Use Rights in Splunk Extensions are limited to your use solely in connection with the applicable Offering and subject to the same terms and conditions for that Offering, unless a Splunk Extension is expressly provided under an Open Source Software license that provides broader rights in that Splunk Extension than the Use Rights you have in the underlying Offering. Despite anything to the contrary in these General Terms, and unless otherwise required by law, Splunk Extensions (excluding Splunk Extensions designated by us as premium) are provided "AS-IS" without any indemnification or warranties. Support and service levels for Splunk Extensions are as set out in the Support Terms.

- Trial, Beta, Test and Similar Offerings

o Trials and Evaluations. We may make certain Trial Offerings available to you under these General Terms. After the Term for the Trial Offering expires, you may continue to use that Offering only subject to payment of applicable Fees.

o Beta Offerings. We may make certain Beta Offerings available to you under these General Terms. Your Use Rights in any Beta Offering are further limited to your use solely for internal testing and evaluation of that Beta Offering during the period specified with the Beta Offering, and if no period is specified, then for the earlier of one year from the Beta Offering start date or when that version of the Beta Offering becomes generally available. We may discontinue a Beta Offering at any time and may decide not to make a Beta Offering or any of its features or functionality generally available.

o Test and Development Offerings. For Offerings identified as "Test and Development" on the Order, your Use Rights are further limited to your use of those Offerings on a non-production system for non-production uses only, including product migration testing or pre-production staging, or testing new data sources, types, or use cases.

o Free Offerings. We may make certain Offerings available for full use (i.e., not subject to limited evaluation purposes) at no charge under these General Terms. These free Offerings may have limited features, functions, and other technical Use Rights limitations.

o Limitations and Termination. Despite anything to the contrary in these General Terms, and unless otherwise stated in the Order or required by law, Trial Offerings, Beta Offerings, Test and Development and any free Offerings are provided "AS-IS" without any indemnification, warranties, maintenance, support or service level commitments. Unless otherwise stated in the Order, we reserve the right to terminate any Offering in this section 1.4 at any time without prior notice and without any liability.

- Specific Offering Terms. Specific security controls and certifications, data policies, service descriptions, Service Level Schedules and other terms specific to Offerings ("Specific Offering Terms") are at http://www.splunk.com/SpecificTerms (which are incorporated by reference). We may change the Specific Offering Terms at any time and without notice, provided these changes will only apply to the Offerings ordered or renewed after the date of the change.

- Interoperability Requirements. If required by law, we will promptly provide the information you request to achieve interoperability between applicable Offerings and another independently created program on terms that reasonably protect our proprietary interests.

2. Purchasing Through Approved Sources

- Splunk Affiliate Distributors. We have appointed certain Splunk Affiliates as our non-exclusive distributors of the Offerings (each, a "Splunk Affiliate Distributor"). Each Splunk Affiliate Distributor is authorized by us to negotiate and enter into Orders with customers. Where a purchase is offered by a Splunk Affiliate Distributor, you will order from, and make payments to, that Splunk Affiliate Distributor. Each Order will be deemed a separate contract between you and the relevant Splunk Affiliate Distributor and will be subject to these General Terms. You agree that: (i) Splunk's total liability under these General Terms as set out in section 20 (Limitation of Liability) states the overall combined liability of Splunk and our Splunk Affiliate Distributors; (ii) entering into Orders by a Splunk Affiliate Distributor will not be deemed to expand Splunk and its Affiliates' overall responsibilities or liability under these General Terms; and (iii) you will have no right to recover more than once from the same event. We agree that: (a) the Splunk Affiliate Distributor will be liable for the performance of the Order; and (b) to the extent that any obligations of the Order are to be performed by us, the Splunk Affiliate Distributor will be responsible for, and ensure our compliance with, the terms of the Order.

- Approved Sources. These General Terms will govern any Offering that you acquire through any Approved Source. Your payment obligations (if any) will be with the Approved Source through whom you acquired the Offering. However, a breach of your payment obligations with any Approved Source for any Offering will be deemed to be a material breach of these General Terms between you and Splunk. In addition, if you fail to pay a Digital Marketplace for an Offering, we retain the right to enforce your payment obligations and collect directly from you. Any terms agreed between you and an Approved Source (other than us or a Splunk Affiliate Distributor) that are in addition to these General Terms are solely between you and that Approved Source. No agreement between you and that Approved Source is binding on us or will have any force or effect with respect to the rights in, or the operation, use or provision of, any Offering.

3. Your Third Party Providers

You may permit your Third Party Providers to access and use the Offerings on your behalf, provided that: (i) such access and use will at all times be subject to these General Terms and any applicable Order; (ii) you will ensure these Third Party Providers comply with these General Terms and any applicable Order; (iii) you are liable for any action or omission of any Third Party Provider if that action or omission would constitute a breach of these General Terms or any Order if done by you; and (iv) the aggregate use by you and all of your Third Party Providers must not exceed the Capacity.

4. Hosted Services

- Service Levels. When you purchase Hosted Services, we will make the applicable Hosted Services available to you during the Term in accordance with these General Terms. The Service Level Schedule in the Specific Offering Terms and associated remedies will apply to the availability and uptime of the applicable Hosted Service. If applicable, service credits will be available for downtime in accordance with the Service Level Schedule.

- Your Responsibility for Data Protection. You are responsible for: (i) selecting from the security configurations and security options made available by Splunk in connection with a Hosted Service; (ii) taking additional measures outside of the Hosted Service to the extent the Hosted Service does not provide the controls that may be required or desired by you; and (iii) routine archiving and backing up of Customer Content. You agree to notify Splunk promptly if you believe that an unauthorized third party may be using your accounts or if your account information is lost or stolen.

- Return of Customer Content. You may retrieve and remove Customer Content from the Hosted Services at any time during the Term. We will also make the Customer Content available for your retrieval for 30 days after termination of your subscription. After those 30 days, we will delete all remaining Customer Content without undue delay, unless legally prohibited. If you require assistance in connection with migration of Customer Content, we may require a mutually agreed upon fee for it.

5. Data Protection

We will follow globally recognized data protection principles for the processing of personal data as described in the applicable data processing addendum at https://www.splunk.com/en_us/legal/splunk-dpa.html (which is incorporated by reference). If we have separately executed a data processing addendum between us covering the same scope, it will apply instead of any data processing addendum posted online.

6. Security

- Security Program. We have implemented and will maintain an industry standard security program to protect our Offerings, IT systems, facilities and assets, and any Customer Confidential Information accessed or processed therein, including Customer Content in a Hosted Service and customer account information. Our Hosted Service security controls include commercially reasonable administrative, technical, and organizational safeguards designed to protect Customer Content against destruction, loss, alteration, unauthorized disclosure, or unauthorized access, such as threat and vulnerability management, incident response and breach notification procedures, disaster recovery plans, open source security scans, virus detection, industry-standard secure software development practices, and internal and external penetration testing in the development environment. Our general corporate security controls include information security policies and procedures, security awareness training, physical and environmental access controls, and vendor risk management.

- Security Exhibits. The specific security measures applicable to certain Offerings are described in the security exhibits at https://www.splunk.com/en_us/legal/splunk-security-addenda.html.

- Maintaining Protections. Despite anything to the contrary in these General Terms or any policy or terms referenced in these General Terms via hyperlink, we may update Security Exhibits from time to time, provided those updates do not materially diminish the overall security protections set out in these General Terms, applicable Specific Offering Terms or Security Exhibits.

7. Support and Maintenance

The specific Support Program included with an Offering will be identified in the Order. We will provide the purchased level of support and maintenance services for an Offering in accordance with the Support Terms effective on the Delivery of that Offering.

8. Configuration and Implementation Services

We offer additional services to configure and implement your Offering (“C&I Services”). These C&I Services are purchased under a Statement of Work and are subject to payment of applicable Fees. We provide C&I Services in accordance with our standard C&I Services terms at https://www.splunk.com/en_us/legal/professional-services-agreement.html, effective on the start date of the Statement of Work.

9. Our Compliance, Ethics and Corporate Responsibility

- Compliance. We will comply with the laws and regulations applicable to our business and the provision of the Offerings to our customers generally, and without regard to your particular use of the Offering.

- Ethics and Corporate Responsibility. We are committed to acting ethically and in compliance with applicable law, and we have policies and guidelines in place to provide awareness of, and compliance with, the laws and regulations that apply to our business globally. We are committed to ethical business conduct, and we use diligent efforts to perform in accordance with the highest global ethical principles, as described in the Splunk Code of Business Conduct and Ethics at https://www.splunk.com/en_us/pdfs/legal/code-of-business-conduct-and-ethics.pdf.

- Anti-Corruption. We implement and maintain programs for compliance with applicable anti-corruption and anti-bribery laws. Our policy prohibits offering or soliciting any illegal or improper bribe, kickback, payment, gift, or thing of value to or from any of your employees or agents in connection with these General Terms. If we learn of any violation of the above, we will use reasonable efforts to promptly notify you at the main contact address that you have provided to us.

- Export. We certify that we are not on any of the relevant U.S. or EU government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. Export information regarding our Offerings, including our export control classifications for our Offerings, is at https://www.splunk.com/en_us/legal/export-controls.html.

- Environmental, Social and Governance. Our positions and commitments on environmental, social and governance aspects of our business, including our Global Impact Reports and ESG Position Statement, are in our ESG Resource Center at https://www.splunk.com/en_us/global-impact/esg-resources.html.

10. Usage Data

We collect and process Usage Data as set out in Splunk's Privacy Statement at https://www.splunk.com/en_us/legal/privacy/privacy-policy.html. Usage Data does not include Customer Content and will be kept confidential.

11. Capacity and Usage Verification

- Certification and Verification. Upon our request, you will provide us with a certification signed by your authorized representative verifying that your use of the Offering is in accordance with these General Terms and any applicable Order. For On-Premises Products, we may also ask you from time to time, but not more frequently than once every 12 months, to cooperate with us to verify usage and adherence to the Capacity. If we request such a verification, you agree to provide us reasonable access to the On-Premises Product installed at your facility (or as hosted by your Third-Party Provider). If we do any verification, it will be performed with as little interference as possible to your use of the On-Premises Product and your business operations. We will comply with your (or your Third-Party Providers') reasonable security procedures.

- Overages. If a verification or usage report reveals that you have exceeded the Capacity or Use Rights, then we will have the right to invoice you using the applicable Fees at list price then in effect, which will be payable in accordance with these General Terms. Except where you have paid the applicable Approved Source for such additional Capacity or Use Rights, we will have the right to directly invoice you for overages, regardless of whether you acquired the Offering from us or another Approved Source.

12. Our Use of Open Source

Certain Offerings may contain Open Source Software. In the applicable Documentation, we make available a list of Open Source Software and applicable licenses incorporated in our On-Premises Products to the extent required by the respective Open Source Software licenses. Any Open Source Software that is delivered as part of your Offering and which may not be removed or used separately from the Offering is covered by the warranty, support and indemnification provisions applicable to the Offering, but only to the extent that Open Source Software is used as intended with the Offering. Some of the Open Source Software may have additional terms that apply to the use of the Offering (e.g., the obligation for us to provide attribution of the specific licensor), and those terms will be included in the Documentation. However, those terms will not: (i) impose any additional restrictions on your use of the Offering; or (ii) negate or amend our responsibilities with respect to the Offering.

13. Third Party Extensions, Content and Products

- Third Party Extensions on Splunkbase. We may make Third Party Extensions available from Splunkbase. We do not represent, warrant or guarantee the accuracy, integrity, quality, or security of any Third Party Extension, even if that Third Party Extension is identified as "certified" or "validated" for use with the Offering. Your use of a Third Party Extension may be subject to additional terms, conditions or policies. We may block or disable access to a Third Party Extension at any time.

- Third Party Content. Hosted Services may contain features that enable interoperation with Third Party Content that you choose to add to a Hosted Service. You may be required to: (i) separately obtain access to Third Party Content from its provider; and (ii) grant us access to your accounts with those providers. By choosing to enable such interoperation by allowing us to enable access to Third Party Content, you: (a) certify that you are authorized to do so; and (b) authorize us to allow that provider to access Customer Content as necessary for interoperation. We are not responsible or liable for disclosure, modification or deletion of Customer Content resulting from such interoperation, nor are we liable for damages or downtime or other impact on the Hosted Service, resulting directly or indirectly from your use of or reliance on Third Party Content, sites or resources.

- Splunk as a Reseller. When you purchase third party products ("Third Party Products") from us as specified in an Order (which products will include third party software, but not any support which we have contracted to provide), the following applies. We act solely as a reseller of Third Party Products, which are fulfilled by the relevant third party vendor, and purchase and use of Third Party Products is subject solely to the terms, conditions and policies made available by that third party vendor. Consequently, we make no representation or warranty of any kind regarding the Third Party Products, whether express, implied, statutory or otherwise, and specifically disclaim all implied terms, conditions and warranties (including as to quality, performance, availability, fitness for a particular purpose or non-infringement) to the maximum extent permitted by applicable law. You will bring any claim in relation to Third Party Products against the applicable third party vendor directly. In no event will we be liable to you for any claim, loss or damage arising out of the use, operation or availability of any Third Party Product (whether such liability arises in contract, negligence, tort, or otherwise).

14. Your Compliance

- Lawful Use of Offerings.When you access and use an Offering, you are responsible for complying with all laws, rules, and regulations applicable to your access and use. This includes, without limitation, being responsible for your Customer Content and users, their compliance with these General Terms, how you acquired your Customer Content, and the accuracy and lawful use of your Customer Content.

- PHI, PCI Data and ITAR Data. You may not transmit or store PHI, PCI Data or ITAR Data within a Hosted Services unless you have specifically acquired an Offering for that applicable regulated Hosted Services environment.

- Registration. You agree to provide accurate and complete information when you register for and use an Offering and agree to keep this information current. Each person who uses an Offering must have a separate username and password. For Hosted Services, you must provide a valid email address for each person authorized to use your Hosted Services. We may require additional information for certain Offerings (e.g., technical information necessary for your connection to a Hosted Service), and you will provide this information as we reasonably request. You are responsible for securing, protecting, and maintaining the confidentiality of your account usernames, passwords and access tokens.

- Export Compliance. You will comply with all applicable export laws and regulations of the United States (which apply irrespective of the use location of the Offerings) and any other country ("Export Laws") where your users use any of the Offerings. You certify that you are not on any of the relevant U.S. government lists of prohibited persons, including the Treasury Department's List of Specially Designated Nationals and the Commerce Department's List of Denied Persons or Entity List. You will not export, re-export, ship, transfer or otherwise use the Offerings in any country subject to an embargo or other sanction by the United States, including, without limitation, Iran, Syria, Cuba, the Crimea Region of Ukraine, Sudan and North Korea, and you will not use any Offering for any purpose prohibited by the Export Laws.

- Acceptable Use. For any Hosted Services, you will also abide by our Hosted Services Acceptable Use Policy at https://www.splunk.com/view/SP-CAAAMB6.

- GovCloud Services. This section 14.6 will apply to you if you access or use any Hosted Services in the specially isolated AWS GovCloud (U.S.) region (including without limitation any Hosted Services that are provisioned in a FedRAMP authorized environment within the AWS GovCloud (U.S.) region)). You hereby represent and warrant that: (i) you are a "U.S. Person" as defined under ITAR (see 22 CFR part 120.62); (ii) you have and will maintain a valid Directorate of Defense Trade Controls registration, if required by ITAR; (iii) you and your end users are not subject to export control restrictions under U.S. export control laws and regulations (i.e., users are not denied or debarred parties or otherwise subject to sanctions); (iv) you will maintain an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including ITAR, as applicable; and (v) you will maintain effective access controls as described in the Specific Offering Terms for the applicable Hosted Services. You are responsible for verifying that any user accessing Customer Content in the Hosted Services in the AWS GovCloud (U.S.) region is eligible to access such Customer Content. The Hosted Services in the AWS GovCloud (U.S.) region may not be used to process or store classified data. You will be responsible for all sanitization costs incurred by us if users introduce classified data into the Hosted Services in the AWS GovCloud (U.S.) region. You may be required to execute additional addenda to these General Terms before provisioning of selected Hosted Services.

15. Confidentiality

- Confidential Information. Each party will protect the Confidential Information of the other. Accordingly, receiving party agrees to: (i) protect disclosing party's Confidential Information using the same degree of care (but in no event less than reasonable care) that it uses to protect its own Confidential Information of a similar nature; (ii) limit use of disclosing party's Confidential Information to only for purposes consistent with these General Terms; and (iii) use commercially reasonable efforts to limit access to disclosing party's Confidential Information to its employees, contractors, agents, or Affiliates, each of which has a bona fide need to access such Confidential Information for purposes consistent with these General Terms, and who are subject to confidentiality obligations no less stringent than those set out here.

- Compelled Disclosure of Confidential Information. Despite the provisions above, receiving party may disclose Confidential Information of disclosing party if it is compelled by law enforcement agencies or regulators to do so, provided receiving party gives disclosing party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at disclosing party's cost, if disclosing party wishes to contest the disclosure. If receiving party is compelled to disclose disclosing party’s Confidential Information as part of a civil proceeding to which disclosing party is a party, and disclosing party is not contesting the disclosure, disclosing party will reimburse receiving party for its reasonable cost of compiling and providing secure access to such Confidential Information.

16. Payment

- Payment Terms. The payment terms in this section 16 only apply when you purchase Offerings directly from us.

- Fees. You agree to pay all Fees specified in the Orders. Fees are non-cancelable and non-refundable, except as otherwise expressly stated in these General Terms. Without limiting any of our other rights or remedies, overdue charges may accrue interest monthly at the rate of 1.5% of the then-outstanding unpaid balance, or the maximum rate permitted by law, whichever is lower. Fees are due and payable either within 30 days from the date of our invoice or as otherwise stated in the Order.

- Credit Cards. For e-commerce transactions, if you choose to pay by credit or debit card, then you: (i) will provide us or our designated third party payment processor with valid credit or debit card information; and (ii) authorize us or our designated third party payment processor to charge such credit or debit card for all items listed in the applicable Order. Such charges must be paid in advance or in accordance with any different billing frequency stated in the applicable Order. You are responsible for providing complete and accurate billing and contact information and notifying us in a timely manner of any changes to such information.

- Taxes.Fees are exclusive of applicable taxes and duties, including any applicable sales and use tax. You are responsible for paying any taxes or similar government assessments (including, without limitation, value-added, sales, use or withholding taxes). We will be solely responsible for taxes assessable against us based on our net income, property, and employees.

17. Warranties

- Relationship to Applicable Law. You may have legal rights in your country that prohibit or restrict the limitations set out in this section 17, which applies only to the extent permitted under applicable law.

- General Corporate Warranty. Each party warrants that it has the legal power and authority to enter into these General Terms.

- Hosted Services Warranty. We warrant that during the Term: (i) we will not materially decrease the overall functionality of the Hosted Services; and (ii) the Hosted Services will perform materially in accordance with the Documentation. For any breach of these warranties, our entire liability, and your sole remedy, will be for us to: (a) modify or correct the Hosted Service so that it conforms to the foregoing warranty; or (b) if we determine that (a) is not commercially, technically or operationally reasonable, terminate the non-conforming Hosted Service, and refund to you any prepaid but unused Fees for the remainder of the Term.

- On-Premises Product Warranty. We warrant that for a period of 90 days from its Delivery, the On-Premises Product will substantially perform the material functions described in the Documentation, when used in accordance with the Documentation. For any breach of this warranty, our entire liability, and your sole remedy, will be for us to: (i) modify, or provide an Enhancement for, the On-Premises Product so that it conforms to the foregoing warranty; (ii) replace your copy of the On-Premises Product with a copy that conforms to the foregoing warranty; or (iii) if we determine that (i) or (ii) is not commercially, technically or operationally reasonable, terminate the Offering with respect to the non-conforming On-Premises Product and refund to you the Fees paid for such non-conforming On-Premises Product.

- Disclaimer of Implied Warranties. Except as expressly set out above, and to the extent allowed by law, the Offerings are provided "AS IS" with no other warranties or representations whatsoever express or implied. We and our suppliers and licensors disclaim all warranties and representations not expressly set out above, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, noninfringement, or quiet enjoyment, and any warranties arising out of course of dealing or trade usage. We do not warrant that use of Offerings will be uninterrupted, error free or secure, or that all defects will be corrected.

18. Ownership

- Offerings. As between you and us, we own and reserve all right, title, and interest in and to the Offerings and other Splunk materials, including all Intellectual Property Rights therein. We retain rights in anything delivered or developed by us or on our behalf under these General Terms. No rights are granted to you other than as expressly set out in these General Terms.

- Customer Content. You own and reserve all right, title and interest in your Customer Content. By sending Customer Content to a Hosted Service, you grant us a worldwide, royalty free, non-exclusive license to access and use the Customer Content for purposes of providing you the Hosted Service and as set out in the Specific Offering Terms. Subject to section 18.1, you own any reporting results that you or your Third Party Providers may derive from Customer Content through the use of the Offerings.