Exhibit D, F, G

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

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.

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

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:

Service Level Agreement for Hosted Services This Service Level Agreement ("SLA") between Tenable ("Tenable") and Customer is subject to the applicable license or subscription agreement between Tenable and Customer under which the Customer licenses the Hosted Services, or if the parties have not executed such separate agreement, the Tenable Master Agreement located at http://static.tenable.com/prod_docs/tenable_slas.html (the "Agreement"). All defined terms used in this SLA and not defined herein shall have the meaning assigned to them in the Agreement. Tenable shall provide the Hosted Services and Software in connection with the Agreement. This SLA governs Tenable's performance and delivery of the Hosted Services to Customer.

1. Definitions.

"Potential Uptime" means the amount of time in a given month. "Production Uptime" represents the amount of time in a given month that Customer has the ability to log in or access the Hosted Services user interface (or authenticate to APIs) and perform associated Scanning related activity. Potential Uptime is measured by Tenable in a given month by the following calculation: Production Uptime = (Potential Uptime – Hosted Services Interruption Time) / (Potential Uptime – Exclusions) "Hosted Services Interruption Time" is the period of time for which the Hosted Services (or any material portion thereof) are unavailable due to issues caused by or attributable to Tenable or its agents. Hosted Services Interruption Time does not include Regular Maintenance or Scheduled Maintenance. "Regular Maintenance" is the period of time under which the Hosted Services may be unavailable for recurring maintenance work. Tenable attempts to schedule this time when usage of the Hosted Services is light across Tenable's customer base and therefore, Tenable shall use commercially reasonable efforts to only conduct Regular Maintenance daily between the hours of 7AM and 9AM (ET) and non-business days. Regular Maintenance is required in order to update Tenable's plug-in databases as well as to maintain system health requirements. Tenable shall use commercially reasonable efforts to minimize any Regular Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Regular Maintenance. "Scheduled Maintenance" is the period of time under which the Hosted Services may be unavailable for non-recurring maintenance. Scheduled Maintenance is required in order to provide updates to the Hosted Services as well as to maintain system health requirements. Tenable shall provide Customer at least twelve (12) hours advance notice prior to Scheduled Maintenance; provided, however, Tenable shall endeavor to provide at least twenty-four (24) hours advanced notice for Scheduled Maintenance. Notice for Scheduled Maintenance will be provided at the following URL or successor location: status.tenable.com. Tenable shall use commercially reasonable efforts to minimize any Scheduled Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Scheduled Maintenance. "Emergency Maintenance" describes maintenance for certain emergency situations, where

advance notice may be not be feasible, possible or practical. Tenable shall use commercially reasonable efforts to minimize any Emergency Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Periods of Emergency Maintenance shall be included in Hosted Services Interruption Time. Tenable Confidential and Proprietary SLA v.3

2. Service Levels Commitment. Tenable commits to provide a 99.95% Production Uptime with respect to the Hosted Services during each calendar month of the subscription term.

3. Service Level Credits. If Tenable fails to perform the Hosted Services in accordance with the Service Level Commitment, then Customer may request a Service Level Credit in accordance with this SLA. Service Level Credits shall be Customer's sole and exclusive remedy for unavailability or performance degradation of the specific Hosted Services.

4. Weighting Factor. The "Weighting Factor" for calculation of the Service Level Credit is set forth below and correlates to the relative unavailability of the Hosted Service in a given month.

Production Uptime between 99.95% and 100% = 0 Production Uptime between 95.00% and 99.94% = .1 Production Uptime between 90.00% and 94.99% = .15 Production Uptime below 90% = .2

5. Calculation of Service Level Credits. The following equation shall be used to calculate any Service Level Credits: Service Level Credit (in $) = Weighting Factor multiplied by the monthly fee for applicable Hosted Service.

Example: Production Uptime in a given month is 95%. The monthly fee for the Hosted Service is $100 (Annual fee for the Hosted Services is $1,200). Service Level Credit (in $) = (0.1) x $100 = $10.

If Customer has paid in advance for one or more years of the Hosted Services, monthly fees will be calculated on a pro rata basis.

6. Exclusions. "Exclusions" shall mean any time for which the Hosted Services are unavailable to do any of the following: (i) Customer's breach of, or failure to perform any obligations under, this SLA or the Agreement; (ii) issues relating to Customer's environment, internal networks, computer systems, firewalls or Customer's inability to connect to the internet; (iii) Force Majeure Events; or (iv) issues arising from failures, acts or omissions Tenable's upstream service providers (i.e. AWS).

7. Requests. In order to receive a Service Level Credit, Customer must request such by emailing Tenable at credits@tenable.com, within 10 days of the end of the applicable month. If Customer is past due or in default with respect to any payment or any material contractual obligations to Tenable, Customer is not eligible for any Service Level Credit. Service Level Credits are non-refundable and may only be applied to future upgrades or renewals of the specific Tenable Hosted Services affected.

8. Changes. This Service Level Commitment may be amended by Tenable in its reasonable discretion but only after providing thirty (30) days' advance notice. Tenable may provide such notice either as a note on the screen presented upon logging in to the Hosted Services, by posting updated terms on Tenable's website, or by email to the email addressed registered with Customer's account. This SLA was updated on October, 2023 (ver 3).

Master Agreement, accepted via a click-thru acknowledgement at time of installation:

Due to the document exceeding the allotted character limit, the full documentation can be located at https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf . We have included what we can below.

TENABLE MASTER AGREEMENT This Master Agreement (this “Agreement”) is made by and between Tenable (as defined below) and the customer licensing Products and/or receiving services (“Customer”) with an effective date as of the date Customer clicks to accept this Agreement (the “Effective Date”). Hereinafter, each of Tenable and Customer may be referred to collectively as the “Parties” or individually as a “Party”.

1. Definitions. (a) “Affiliate” means any entity that controls, is controlled by, or is under common control with a Party. “Control” shall mean: (1) ownership (either directly or indirectly) of greater than fifty percent (50%) of the voting equity or other controlling equity of another entity; or (2) power of one entity to direct the management or policies of another entity, by contract or otherwise. (b) “Documentation” means the then-current official user manuals and/or documentation for the Products available at docs.tenable.com (or a successor location). (c) “Hosted Services” are a type of service offered through Tenable’s cloud-based software as a service (SaaS) platform and include Scans and access to and use of the hosted environment (the “Hosted Environment”). (d) “Product(s)” means any of the products that Tenable offers, including Software, Hosted Services, Hardware (if any), Support Services and Professional Services. (e) “Professional Services” means services purchased, including consulting services which are relevant to the implementation and configurations of Tenable Products as well as on-site or virtual training courses. Generally, Professional Services are defined either in a separate SOW or a Services Brief. Professional Services do not include the Hosted Services or Support Services. (f) “Scan(s)” are a function performed by the Software and/or the Hosted Services on Scan Targets, which are conducted in order to provide data to Customer regarding its network security. “PCI Scans” are a specific type of Scan designed to assess compliance with the Payment Card Industry Data Security Standard. “Scan Data” is the resulting information created by the Scan. “Scan Target(s)” are the targets or subjects of a Scan. (g) “Services Brief” means the document which outlines Tenable’s basic, pre-packaged installation or training Professional Services offered under a Tenable SKU and which do not require a separate SOW. Current versions of Services Briefs may be found at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). For the avoidance of doubt, Customer may purchase commercial off the shelf SKU-based Professional Services without executing a separate Statement of Work. A “SOW” or “Statement of Work” shall further describe Professional Services, the terms of which may be customized and which shall require execution by the Customer. (h) “Software” means each software product made available by Tenable under this Agreement for download. Software includes patches, updates, improvements, additions, enhancements and other modifications or revised versions of the same that may be provided to Customer by Tenable from time to time. (i) “Technical Data” means data Customer uploads or runs through or on the Products, or is otherwise generated thereby, including information regarding licensing metrics and product behavioral data. (j) “Tenable” means: (i) Tenable, Inc., if Customer is a commercial entity or individual located in North or South America (Tenable, Inc. is a Delaware corporation having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); (ii) Tenable 2 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 Public Sector LLC, if Customer is an agency or instrumentality of the United

States Government, a commercial entity operating predominantly as a federal systems integrator for eventual sale or resale or for the benefit of the United States Government, or an agency or instrumentality of a State or local government within the United States (Tenable Public Sector LLC is a Delaware limited liability company having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); or (iii) Tenable Network Security Ireland Limited, if Customer is located outside of North or South America (Tenable Network Security Ireland Limited is a private limited company having offices at 81b Campshires, Sir John Rogerson's Quay, Dublin 2, Ireland).

2. Orders and Transactions. (a) Reseller Transactions. If Customer purchases Tenable Products through an authorized Tenable reseller (a "Reseller"), all terms related to pricing, billing, invoicing and payment ("Payment Terms") set forth in this Agreement (if any) shall not apply. For the avoidance of doubt, all such Payment Terms shall be as agreed to between Customer and Reseller. To place an order, Customer shall provide the Reseller with a purchase order (or other similar document acceptable to Reseller) in response to a valid quote from such Reseller. Following Reseller's receipt of such purchase order, Tenable shall issue a sales order confirmation or other similar order acceptance document (the "Ordering Document"). No order shall be deemed accepted by Tenable until Tenable issues the Ordering Document. The Ordering Document shall set forth all Products (and corresponding licensing metrics) purchased by Customer. (b) Direct Transactions. If the Parties have agreed to transact directly, the following Payment Terms shall apply. Customer agrees to pay all amounts due as specified in a Tenable invoice. Fees for Hosted Services are charged for access to the Host Environment (as defined herein), not actual usage. Payment is due within thirty (30) days from the date of Tenable's invoice to Customer. Customer will pay directly or reimburse Tenable for any taxes (including, sales or excise taxes, value added taxes, gross receipt taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, imposed on or arising out of this Agreement. Notwithstanding the foregoing, Tenable will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. Customer agrees to pay Tenable without deducting any present or future taxes, withholdings or other charges except those deductions it is legally required to make. If Customer is legally required to make any deductions or withholding, Customer agrees to provide evidence of such withholding upon request. If a certificate of exemption or similar document or proceeding is necessary in order to exempt any transaction from a tax, Customer shall provide such certificate or document to Tenable. (c) Delivery and Installation. Delivery of Tenable Products ("Delivery") shall be deemed to occur on the date of availability for electronic download or electronic access. Tenable has no duty to provide installation services for Tenable Products unless installation services are purchased separately.

3. Term and Termination. (a) Agreement Term. This Agreement shall commence upon the Effective Date and continue until terminated in accordance with the terms set forth herein. (b) License Term and Renewals. The "License Term" is the term of the license or subscription for Products as set forth in the Ordering Document. If this Agreement has been signed by both Parties, then unless otherwise agreed to in writing, any License Term, including renewals, shall be governed by the terms set forth herein. If this Agreement has been accepted via shrinkwrap or click through, upon any renewal of the License Term, the terms then available at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location) will govern such renewal. Customer agrees that use of the Products at the time of such renewal will be deemed full and adequate acceptance of the updated terms. (c) Termination for Cause. Either Party may terminate this Agreement for cause if the other Party materially breaches this Agreement provided that such breaching Party has received written notice of such breach and failed to cure such

breach within thirty (30) days. If this Agreement is terminated for cause by either Party, Customer shall remove all copies of the Products from any Customer systems and cease to use any Software or Hosted Services purchased hereunder. Further, Customer shall certify to Tenable that it has returned or destroyed all copies of the Software. If this Agreement is terminated for cause by Tenable, Customer shall remain responsible for any outstanding payment obligations throughout the rest of the License Term. (d) Termination for Convenience. Customer may terminate this Agreement for any lawful reason upon ninety (90) days' prior written notice to Tenable. If Customer terminates for convenience, Customer shall not receive a refund and shall remain obligated to pay for Products for which it has previously entered into a transaction as well as any additional payment obligations agreed upon prior to the termination date.

4. Products. (a) Product-Specific Terms. Pursuant to this Agreement, Customer may receive the right to use various Products as further described in the attached schedules (each, a "Schedule"). Terms related to Customer's use of Software are described in Schedule A 3 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 (Software). Terms related to Customer's use of Hosted Services are described in Schedule B (Hosted Services). Terms related to the provision of Professional Services are described in Schedule C (Professional Services). For each Product, Customer will have the right to use the corresponding Documentation. (b) Licensing Model. Product licenses shall be in accordance with the terms of the applicable licensing model as set forth in the Documentation and/or the Ordering Document, which may include limitations on Scan Targets, compute, storage, resource utilization, License Term, the number of users, seats, licenses and/or types of modules licensed. Product licenses shall commence upon Delivery and shall be either perpetual or subscription in nature. Tenable shall use commercially reasonable efforts to meter resource utilization and assess likeness or uniqueness of Scan Targets within each Product/module licensed. If Customer exceeds the license restrictions, Customer must purchase an upgraded license to allow for all actual or additional usage, and Tenable or its Reseller may promptly invoice Customer for any such overages at a price not to exceed Tenable's then-current rates. Discrepancies in Scan Target or utilization count is the sole responsibility of the Customer to resolve. (c) Restrictions on Use. Customer shall not directly or indirectly: (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive, obtain or modify the source code of the Products; (ii) reproduce, modify, translate or create derivative works of all or any part of the Products; (iii) remove, alter or obscure any proprietary notice, labels, or marks on the Products; (iv) without Tenable's prior written consent, use the Products in a service bureau, application service provider or similar capacity; (v) without signing Tenable's Managed Security Services Provider Addendum, use the Products to provide any managed service to a third party; (vi) use the Products in order to create competitive analysis or a competitive product or service; (vii) copy any ideas, features, functions or graphics in the Product; or (viii) without Tenable's prior written consent, interfere with or disrupt performance of Hosted Services (e.g., perform penetration testing on Tenable systems). Customer may only use the Products to manage or gather information from Scan Targets owned or hosted by Customer or its Affiliates, or third parties for which Customer has received express authorization to Scan. (d) Intellectual Property in Products. This Agreement does not transfer to Customer any title to or any ownership right or interest in the Products. Any rights in the Products not expressly granted in this Agreement are reserved by Tenable. If Customer provides Tenable with any comments, suggestions, or other feedback regarding the Product, Customer hereby assigns to Tenable all right, title and interest in and to such feedback. For clarity, such feedback shall not contain Customer Confidential Information and shall not reference or identify Customer or its users. (e) Customer Requirements.

In order to use the Products, Customer must meet or exceed the specifications found in the Documentation. (f) Product Features. Customer agrees that purchase of any Product is not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Tenable regarding future functionality or features. Tenable reserves the right to withdraw features from future versions of the Products provided that: (i) the core functionality of the affected Product remains the same; or (ii) Customer is offered access to a product or service providing materially similar functionality as the functionality removed from the affected Product. The preceding remedies under this Section 4(f) are the sole remedies available if Tenable withdraws features from the Products. (g) Rights Granted to Tenable. Provided that Tenable shall not publicly disclose any Customer Confidential Information, Tenable may: (i) use Technical Data for reasonable business purposes, including Support Services, license validation, research and development, feature creation, and Product testing; (ii) include aggregated and anonymized Technical Data in public materials; and (iii) retain Technical Data which is anonymized after the termination of this Agreement. (h) Hardware. Any Hardware purchased under this Agreement (if any) will be subject to the terms and conditions of Schedule D located at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). (i) Temporary Limitation. If Tenable reasonably believes: (i) Customer's use of the Products places an unreasonable or disproportionate burden on the Products; (ii) Customer's use of the Products poses a risk or threat to the Products (including any systems supporting the Products), Tenable, or a third party; or (iii) Customer's usage exceeds the limitations of the license, then Tenable may temporarily limit Customer's access to or use of the Products or any specific feature therein. Tenable may also suspend or limit access to the Products if Customer fails to make any payments related to this Agreement. Tenable will, to the extent practical under the circumstances, use commercially reasonable efforts to provide Customer with prior written notice of any such limitation (email or in product messaging shall be sufficient). When commercially reasonable, Tenable shall promptly restore access once the Customer has remediated the issue. For the avoidance of doubt, Customer is responsible for all normal fees during any period for which usage or access is limited pursuant to this section. (j) Additional Details on Use Restrictions for Tenable Security Network Ireland Limited. The following shall only apply for transactions with Tenable Security Network Ireland Limited. Notwithstanding anything in Section 4(c), decompiling the Product is 4 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 permitted to the extent the laws of Customer's jurisdiction give Customer the right to do so to obtain information necessary to render the Products interoperable with other software; provided, however, that Customer must first request such information from Tenable and Tenable may, in its discretion, either provide such information to Customer or impose reasonable conditions, including a reasonable fee, on such use of the Products to ensure that its proprietary rights in the Product are protected.

5. Support. (a) Support Services. Tenable shall provide Customer with support services (the "Support Services") in accordance with Tenable's then-current Technical Support Plans (available at http://static.tenable.com/prod_docs/tenable_slas.html or a successor location) and consistent with Tenable's End of Life and End of Sale definitions contained therein. The Support Services include bug fixes, updates (including new vulnerability plug-ins), or enhancements that Tenable makes generally available to users of the Products. The Support Services also include the provision of new minor (Example: 1.1.x to 1.2.x, etc.) and major version releases of the Products (Example: 1.x to 2.x, etc.). (b) Support Fees. Standard Support Services for Products licensed for a finite License Term will be provided at no additional charge beyond the license fee for the

duration of the License Term. Support Services for Products licensed on a perpetual basis must be purchased separately in advance. In all cases, premium support may be purchased at an additional charge. If during the course of a perpetual license Customer terminates or fails to renew the Support Services, Customer may, at any time during the term of this Agreement, request that Tenable reinstate the Support Services provided that Customer pays for the lapsed Support Services in an amount equal to the total fees Customer would have paid for the Support Services between the time Customer's Support Services lapsed and the then-current date.

6. Confidentiality. (a) Definition. "Confidential Information" means information learned or disclosed by a Party under this Agreement that should reasonably be assumed to be confidential or proprietary, including the Products and the terms of this Agreement. Confidential Information will remain the property of the disclosing Party, and the receiving Party will not be deemed by virtue of this Agreement or any access to the Confidential Information to have acquired any right, title or interest in or to the Confidential Information. (b) Obligations. Each Party agrees to only use the Confidential Information in connection with this Agreement or a purchase hereunder. The receiving Party agrees to hold the disclosing Party's Confidential Information confidential using at least the same level of protection against unauthorized disclosure or use as the receiving Party normally uses to protect its own information of a similar character, but in no event less than a reasonable degree of care. Each Party may share Confidential Information with its Affiliates or authorized contractors in the performance of its duties under this Agreement; provided, however, that each Party shall be responsible to ensure that such Affiliate or authorized contractors are bound by obligations of confidentiality at least as stringent as those set forth in this Agreement. (c) Exclusions. Confidential Information shall not include information that: (i) is already known to the receiving Party free of any confidentiality obligation; (ii) is or becomes publicly known through no wrongful act of the receiving Party; (iii) is rightfully received by the receiving Party from a third party without any restriction or confidentiality; or (iv) is independently developed by the receiving Party without reference to the Confidential Information. Confidential Information does not include Scan Data that has been aggregated or anonymized so that it is not attributable to the disclosing Party. If Customer requests or performs scans on third party Scan Targets, and such third party inquires with Tenable about the scan, Tenable shall inform Customer and allow Customer to resolve any disputes with the third party. If Customer fails to contact the third party, Customer agrees that Tenable may provide Customer's business contact information to the owner of the Scan Targets as well as to relevant authorities, and such disclosure shall not be considered a breach of confidentiality. (d) Sensitive Information. The Parties agree that Customer's disclosure of sensitive, personal information (e.g., social security numbers, national identity card numbers, personal credit card information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and health care data) ("Sensitive Information") is not required for Tenable to perform its duties under this Agreement or sell any Products hereunder. If Customer inadvertently or unintentionally discloses any Sensitive Information to Tenable, Customer shall identify to Tenable that it has disclosed Sensitive Information and Tenable shall promptly return and/or destroy such Sensitive Information. (e) Legal Disclosures; Remedies. The receiving Party may disclose Confidential Information if required to do so by law provided the receiving Party shall promptly notify the disclosing Party so that the disclosing Party may seek any appropriate protective order and/or take any other action to prevent or limit such disclosure. If required hereunder, the receiving Party shall furnish only that portion of the Confidential Information disclosure of which is legally required. The receiving Party acknowledges and agrees that the breach of any term, covenant or provision of this Agreement

may cause irreparable harm to the disclosing Party and, accordingly, upon the threatened or actual breach by the receiving Party of any term, covenant or provision of this Agreement, the disclosing Party shall 5 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 be entitled to seek injunctive relief, together with any other remedy available at law or in equity. The receiving Party will notify the disclosing Party promptly of any unauthorized use or disclosure of the disclosing Party's Confidential Information.

7. Representations and Warranties; Disclaimer. (a) Warranty of Authority. The Parties hereby represent and warrant that they have the full power and authority to enter into this Agreement. (b) Products. Product warranties and associated warranty periods are set forth in the relevant Schedules. (c) Antivirus Warranty. Tenable represents it has taken commercially reasonable efforts to ensure that the Products, at the time of Delivery, are free from any known and undisclosed virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that would erase data or programming or otherwise cause the Products to become inoperable or incapable of being used in the manner for which it was designed or in accordance with the Documentation. (d) Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT AND TO THE GREATEST EXTENT PERMITTED BY LAW, TENABLE OFFERS ITS PRODUCTS "AS-IS" AND MAKES NO OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF TITLE, NON INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SECURITY, INTEGRATION, PERFORMANCE AND ACCURACY, AND ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. THE WARRANTIES SET FORTH IN THIS AGREEMENT ARE MADE TO CUSTOMER FOR CUSTOMER'S BENEFIT ONLY. CUSTOMER'S USE OF THE PRODUCTS IS AT CUSTOMER'S OWN RISK. CUSTOMER UNDERSTANDS THAT ASSESSING NETWORK SECURITY IS A COMPLEX PROCEDURE, AND TENABLE DOES NOT GUARANTEE THAT THE RESULTS OF THE PRODUCTS WILL BE ERROR-FREE OR PROVIDE A COMPLETE AND ACCURATE PICTURE OF CUSTOMER'S SECURITY FLAWS, AND CUSTOMER AGREES NOT TO RELY SOLELY ON SUCH PRODUCTS IN DEVELOPING ITS SECURITY STRATEGY. CUSTOMER ACKNOWLEDGES THAT THE PRODUCTS MAY RESULT IN LOSS OF SERVICE OR HAVE OTHER IMPACTS TO NETWORKS, ASSETS OR COMPUTERS (INCLUDING MODIFICATION OF SCAN TARGETS), AND CUSTOMER IS SOLELY RESPONSIBLE FOR ANY DAMAGES RELATING TO SUCH LOSS OR IMPACT.

8. Limitation of Liability. (a) Direct Damages. The cumulative liability of one Party to the other for all claims arising from or relating to the Products or this Agreement (including without limitation, any cause of action sounding in contract, tort or strict liability) shall be limited to proven direct damages in an amount not to exceed, in the aggregate, the fees paid by Customer for the Products over the twelve (12) months immediately prior to the event giving rise to the claim. (b) Indirect Damages. Neither Party shall be liable to the other for any indirect, incidental, special, punitive, consequential or exemplary damages regardless of the nature of the claim. This prohibition on indirect damages shall include, but not be limited to, claims based on lost profits, cost of delay, any failure of Delivery, business interruption, cost of lost or damaged data, or liabilities to any third parties even if such Party is advised of the possibility thereof. (c) Carve Outs. The liability caps set forth in Sections 8(a) and 8(b) shall not apply to damages resulting from: (i) personal injury or death; (ii) fraud or willful misconduct; (iii) indemnification obligations set forth in Section 9 (Indemnification); or (iv) Customer's breach of Section 4(c) (Restrictions on Use). (d)

Limitations; Time Period. Each of the limitations set forth in this Section 8 shall be enforced to the fullest extent of the law. Any laws preventing such limitations shall only apply to the extent required by law and the remaining unaffected terms shall apply in full. Unless expressly prohibited by law, each Party shall have a period of no greater than twelve (12) months from the date the cause of action accrues to bring a claim against the other Party for such cause of action.

9. Indemnification. (a) Indemnification Obligations. (i) By Tenable. Tenable shall (at its sole cost and expense): (i) defend and/or settle on behalf of Customer (including Customer's officers, directors, employees, representatives and agents); and (ii) indemnify Customer for, any third party claims brought 6 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 against Customer based upon a claim that Customer's use of the Products in accordance with this Agreement infringes or misappropriates such third party's intellectual property rights in a jurisdiction which is signatory to the Berne Convention. (ii) By Customer. Customer shall (at its sole cost and expense): (i) defend and/or settle on behalf of Tenable (including Tenable's officers, directors, employees, representatives and agents) and (ii) indemnify Tenable for, any third party claims brought against Tenable arising out of or relating to Customer's use of the Products to perform Scans on third party Scan Targets, except to the extent that any such claim or action is caused by a failure of the Products to materially comply with the Documentation. (b) In Case of Infringement. If Customer's use of the Products is, or in Tenable's opinion is likely to be, the subject of an infringement claim, Tenable may, in its sole discretion and expense: (i) modify or replace the infringing Products as necessary to avoid infringement, provided that the replacement Products are substantially similar in functionality; (ii) procure the right for Customer to continue using the infringing Products; or (iii) terminate this Agreement and, upon Customer's return or certified destruction of the infringing Product, provide Customer a pro-rata refund calculated as follows: (x) for infringing Products licensed on a subscription basis, the refund shall consist of any prepaid but unused fees for the remainder of the applicable License Term; or (y) for infringing Software licensed on a perpetual basis or infringing Hardware, the refund shall consist of a straight line depreciation of the license fee based on a three (3) year useful life as well as any prepaid but unused fees for separately charged Support Services. This Section 9 sets forth Tenable's sole and exclusive liability and Customer's sole and exclusive remedy with respect to any claim of intellectual property infringement. (c) Exclusions. Tenable shall have no liability with respect to a third party intellectual property infringement claim arising out of: (i) modifications of the Product made by Customer or a party under its control to conform with Customer's specifications; (ii) modifications of the Product made by anyone other than Tenable or a Tenable authorized third party; (iii) Customer's use of the Product in combination with other products or services not provided by Tenable; (iv) Customer's failure to use any updated versions of the Product made available by Tenable; or (v) Customer's use of the Product in a manner not permitted by this Agreement or otherwise not in accordance with the Documentation. (d) Requirements. The indemnitor shall only be responsible for the indemnification obligations set forth in this Section 9 if the indemnitee: (i) provides the indemnitor prompt written notice of such action or claim; (ii) gives the indemnitor the right to control and direct the investigation, defense, and/or settlement of such action or claim; (iii) reasonably cooperates with the indemnitor in the defense of such a claim (at the indemnitor's expense); and (iv) is not in breach of this Agreement. Nothing herein shall prevent the indemnitee from engaging in defense of any such claim with its own legal representation, provided that this does not materially prejudice the indemnitor's defense. The indemnitor may not settle any claim on behalf of the indemnitee without obtaining the indemnitee's prior written consent; provided, however, the indemnitor shall not be required to obtain consent to

settle a claim which settlement consists solely of: (x) discontinued use of infringing Products and/or (y) the payment of money for which the indemnitor has a duty to indemnify.

10. Legal Compliance. (a) Generally. The Products are intended solely for lawful purposes and use. Both Parties, and their agents and Affiliates, agree to perform their respective obligations in an ethical manner that complies with all applicable national, federal, state and local laws, statutes, ordinances, regulations and codes ("Applicable Laws") including, without limitation, the Computer Fraud and Abuse Act (CFAA), 18 USC Sec. 1030, the U.S. Foreign Corrupt Practices Act of 1977, as amended, and the UK Bribery Act of 2010. If Customer violates this Section 10, Tenable may terminate this Agreement immediately. (b) Trade Controls. Applicable Laws include U.S. export laws (including the International Traffic in Arms Regulation (ITAR), 22 CFR 120-130, and the Export Administration Regulation (EAR), 15 CFR Parts 730 et seq.) and the anti-boycott rules implemented by the Departments of Commerce and Treasury. Information regarding export classifications of Tenable's Products may be found on its website (www.tenable.com/export-controls or a successor location). Customer agrees that it will be the exporter of record any time it causes the Products to be accessed outside the United States or by a national of any country other than the United States. The Parties further agree to comply with trade and economic sanctions, rules, and regulations of the United States, European Union, EU member states, United Kingdom and other applicable government authorities and shall not engage in prohibited trade to persons or entities who are the subject of an active sanction, embargo, or executive order. Customer hereby acknowledges and confirms that Customer (including Customer's officers, directors, employees, representatives and agents): (i) is not included on, owned or controlled by an individual or entity included on, or acting on behalf of an individual or entity included on any of the restricted party lists maintained by the U.S. Government (e.g., Specially Designated Nationals List, Foreign Sanctions Evader List, Sectoral Sanctions Identification List, Denied Persons List, Unverified List, Entity List or List of Statutorily Debarred Parties) (collectively, "Restricted Parties"); (ii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use by or for Restricted Parties; (iii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use in, by or for countries or territories subject to U.S. economic sanctions (e.g., Crimea, Cuba, Iran, North Korea, or Syria); or (iv) will not use or sell the Products…

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

Solution Name: Zscaler - Zero Trust Network Segmentation

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.

Zscaler's Airgap Zero Trust Device Segmentation (ZDS) is an on-premises, networking solution that extends Zscaler's Zero Trust capabilities all the way down to the individual device level, within the protected VLANs at the client site. The ZDS platform blocks unwanted lateral threats from propagating between the devices located within the same VLAN, or between different layers of the protected network environment. ZDS makes it easy to significantly reduce the threat surface within the protected VLANs.

ZDS is a completely agentless approach that can be deployed quickly, without requiring significant changes to the existing network architecture, routers, firewalls, switch configurations, etc. Because there are no required software agents or external network hardware, the ZDS solution is easy to drop into existing IT/OT environments without disrupting ongoing operations. ZDS micro-segmentation is ideal for dynamic network environments, where it is typically very difficult and cumbersome to deploy and configure ACLs or other static methods to control network flows down to the individual device level.

Zscaler's ZDS is a standards-based solution that works in all types of IP network environments (including: IT/OT/IoT/IIoT). In addition to enforcement of lateral traffic policies, ZDS also offers robust visibility of network endpoints by discovering, identifying, and classifying any IP-connected devices, including critical assets, servers, PLC/DCS, EWS, HMI, cameras, facilities, headless devices, etc. Because ZDS is completely agentless, we can extend our true zero trust protection to a much higher percentage of the critical devices, especially those in restricted networks like OT manufacturing and healthcare environments, where it can be very difficult or impossible to install or deploy endpoint agent software or other tools and methods.

Zscaler's ZDS solution contains a rich set of device discovery, asset identification and classification capabilities, including the option to classify or group devices into subsets, according to device type, location, function, line or other customizable attributes. ZDS can also ingest information from other standard asset identification platforms or EDR agent-based solutions, such as Crowdstrike Falcon. In addition, the ZDS gateway supports a deep library of API drivers available to enable simple integrations with SIEM/SOAR platforms and other popular cybersecurity logging or analysis tools.

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.

Zscaler’s ZDS is an agentless solution deployed without requiring significant changes to the existing network architecture. ZDS sits in-line of all communications to capture any assets communicating on the network. The solution leverages its role as the default gateway for all protected VLANs so that all communication is detected in real time as a byproduct of forwarding network traffic.

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.

ZDS identifies new devices, regardless of endpoint make/model. It includes device discovery, asset identification, and classification, with options to group devices by type, location, function, or other attributes. ZDS acts as an inline gateway in the network topology, functioning as the default gateway for protected VLANs, detecting all traffic in real time. Endpoints communicating on the network, including servers, workstations, VMs, or IoT devices, are observed regardless of characteristics.

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.

ZDS uses a multi-vector approach to deliver robust endpoint identification and classification. Some of these methods include Organizational Unique Identifiers (OUI/reserved MAC address prefixes), application protocol behavior, and DHCP payload inspection. Endpoints can then be classified and reported based on operating system, device manufacturer, device type (workstation, printer, etc), as well as configured settings like IP address.

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.

ZDS provides host inventory, flow logs, flow analytics, and a relationship map view based on IP communication between endpoints. Flows between endpoints show devices that communicate (or attempt to communicate) with each other. The link map is critical to understanding the current threat exposure and relationships varying devices share. Color-coded indicators make it easy to quickly differentiate between normal allowed traffic and prohibited communications which may reflect undesired behavior.

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.

ZDS platform contains a detailed set of device discovery, asset identification and classification capabilities, including the option to classify or group devices into subsets, according to device type, location, function, line or other customizable attributes. The discovery and reporting information enables granular policy management and control, without requiring significant admin overhead or large groups of access lists and other methods that can be very difficult to manage effectively.

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.

When leveraging Zscaler's Client Connector alongside ZDS, the solution can detect and report OS, firmware, and even browser versions that would indicate patching level and misconfigurations that may be policed in the Zero Trust Exchange to allow, block, or isolate requests from those devices.

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.

Zscaler's solution integrates proprietary (ThreatLabz) and third-party CTI feeds from 40+ sources (such as Mandiant and Recorded Future), continuously updated by Zscaler's threat research teams. Using advanced threat intelligence and automated malware analysis, Zscaler's Single Scan Multi Action engine and Sandbox detect and block malicious traffic in near real time, correlating user activity and network behavior with known threats.

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.

Zscaler commits to SLAs with defined service credits and clear performance metrics, ensuring accountability in availability, latency, and security. Specific SLAs include:

- Global Availability: >= 99.999%
- Global Latency: <= 100ms

Zscaler's SLAs cover latency without exclusions for DLP or malware scanning. Violations are subject to penalties as detailed in each product's SLA sheet, available at: http://www.zscaler.com/legal/sla-support. For transparency, we provide reporting on proxy latency and offer a real-time public status page for cloud availability at https://trust.zscaler.com.

Full Details listed at: https://www.zscaler.com/legal/sla-support

Zscaler's services are governed by our End User Subscription Agreement, available at https://www.zscaler.com/legal/end-user-subscription-agreement. While we operate as a multi-tenant cloud provider with standard terms, Zscaler is open to negotiating mutually agreeable terms and conditions upon selection as a vendor.

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

Solution Name: CyberArk - Endpoint Priviledge Manager (EPM)

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.

CyberArk Endpoint Privilege Manager (EPM) offers robust, continuous monitoring of endpoint activities to detect, investigate, and respond to threats in real-time.

1. **Real-Time Monitoring**: EPM continuously tracks endpoint activities, including file access, process execution, network connections, and registry changes. This comprehensive monitoring helps in identifying unusual patterns that may indicate malicious behavior.

2. **Behavioral Analytics**: By analyzing the behavior of applications and users, EPM can detect anomalies that deviate from normal patterns. This includes monitoring for unusual file access patterns, unexpected process executions, and abnormal network connections.

3. **Threat Detection and Response**: EPM uses advanced algorithms to correlate data from various sources, enabling it to detect potential threats quickly. Once a threat is identified, EPM can automatically respond by blocking malicious activities, isolating affected endpoints, and alerting security teams for further investigation.

4. **Data Collection**: EPM collects detailed data on file access patterns, process execution, network connections, and registry changes. This data is crucial for identifying malicious behavior, as it provides a comprehensive view of endpoint activities. By analyzing this data, EPM can detect subtle signs of compromise that might be missed by traditional security measures.

5. **Policy Enforcement**: EPM enforces least privilege policies, ensuring that users and applications only have the permissions they need to perform their tasks. This reduces the attack surface and limits the potential damage from compromised accounts.

6. **Integration with Security Ecosystem**: EPM integrates with other security tools and platforms, enhancing its ability to detect and respond to threats. This integration allows for a more coordinated and effective security strategy.

By leveraging these capabilities, CyberArk EPM provides a comprehensive solution for monitoring and securing endpoints, ensuring that threats are detected and mitigated in real-time.

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.

CyberArk Endpoint Privilege Manager (EPM) provides real-time monitoring and logging of endpoint activities such as file changes, process creation/termination, registry edits, network connections, and USB insertions. It enhances security by identifying and flagging suspicious activities for further investigation and cross-referencing with network security platforms.

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.

CyberArk Endpoint Privilege Manager (EPM) uses behavior analytics to monitor and analyze user activities, identifying potential threats and unusual behavior patterns. And there is a REST API for integrations. It integrates seamlessly with various security tools, including SIEM platforms like Splunk and QRadar, identity management solutions like Microsoft Azure AD, and IT service management tools like ServiceNow.

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.

CyberArk Endpoint Privilege Manager automates threat response by enforcing least privilege and application control. It detects and blocks unauthorized applications, terminates malicious processes, and prevents credential theft. The system can also automatically elevate privileges for trusted applications, ensuring security without disrupting user productivity.

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.

CyberArk Endpoint Privilege Manager queries and detects indications of compromise by analyzing endpoint activities and behaviors. It identifies patterns of advanced threats through real-time monitoring and integrates with CyberArk's Application Risk Analysis Service (ARA), which automatically uncovers sophisticated APTs, zero-day attacks, and targeted threats.

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.

The EPM agent continues to enforce policies, even without available connectivity to EPM services. An Offline Policy Authorization Generator tool is available for EPM administrators to authorize privilege elevation to an endpoint when the service is not available. This tool is a stand-alone executable that enables endpoint users to request one-time use of an application they currently do not have privileges to run if there are issues accessing the service.

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.

CyberArk EPM uses AI logic leverages a machine learning (ML) algorithm that is based on community data industry verticals, market segmentation and best practices, and provides security-oriented advice that is tailored to your enterprise environment.

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.

In addition to CyberArk EPM's Application Risk Analysis Service (ARA), CyberArk EPM integrates with third-party services like **Palo Alto WildFire** and **Check Point ThreatCloud**. These services help detect potential security threats by analyzing applications in sandbox environments, identifying unknown malware, and providing detailed reports on malicious behavior.

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.

CyberArk Endpoint Privilege Manager enables investigation of historic endpoint activities by providing a detailed timeline of events. This timeline helps in identifying patterns and anomalies, allowing for effective root cause analysis of incidents. By tracking user actions and application behaviors, it ensures comprehensive visibility and aids in pinpointing the exact cause of security breaches.

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.

CyberArk Endpoint Privilege Manager uptime SLA is 99.95%

CyberArk Service Availability Service Level Agreement

This Service Availability Service Level Agreement ("SLA") is incorporated into and subject to the CyberArk SaaS Terms of Service (the "SaaS Terms"). Unless otherwise provided herein, all capitalized terms will have the meaning specified in the SaaS Terms. CyberArk reserves the right to change the terms of this SLA from time to time.

Availability Commitment. CyberArk shall use commercially reasonable efforts to make the SaaS Product (excluding any locally installed agents or connectors) (the "Service") available at an Uptime Percentage as set forth in Annex 1 (the "Availability Commitment"). As used herein, "Uptime Percentage" means the total number of minutes in a calendar month minus the number of minutes of Unavailability (excluding Unavailability associated with any SLA Exclusion) incurred in a calendar month, divided by the total number of minutes in a calendar month. "Unavailable" and "Unavailability" are defined per SaaS Product, as set forth in Annex 1. The Availability Commitment of each Service is measured independently.

Service Credits. In the event CyberArk does not meet the Availability Commitment, Customer shall be eligible to receive a credit ("Service Credit"). Service Credits are calculated as a percentage of the pro-rated monthly subscription fee paid to CyberArk for the affected SaaS Product for the Subscription Term in which the Unavailability occurred, and based on the actual Uptime Percentage, as detailed in Annex 1. The receipt of a Service Credit is CyberArk's sole liability and Customer's exclusive remedy for CyberArk's failure to meet the Availability Commitment.

Credit Request. In order to receive a Service Credit, Customer must submit a request that reasonably details the claimed Unavailability, by opening a ticket in CyberArk Customer Portal, within fourteen (14) days following the end of the calendar month in which the Unavailability occurred. CyberArk shall review the request, and if it confirms, acting reasonably and in good faith, that the actual Uptime Percentage of the Service referenced in the request did not meet the Availability Commitment, CyberArk will provide Customer with a Service Credit, applicable against future fees payable by Customer. In the event that Customer does not renew its then-current Subscription Term of the applicable SaaS Product and has no outstanding payments due to CyberArk, then Customer shall be entitled to receive a refund of the Service Credit. A Service Credit may not be transferred to other CyberArk customers.

SLA Exclusions. The Availability Commitment does not apply to any Unavailability arising from (i) factors outside of CyberArk’s reasonable control, including but not limited to, any force majeure event, Internet access, electrical disruptions; (ii) Customer’s network, on-premise environment and related components (including, access to Customer’s hosted encryption keys, operating systems, software and platforms); (iii) any equipment, software or other technology other than those within CyberArk’s direct and sole control; (iv) connectivity issues due to any firewall, censorship infrastructure, internet monitoring tool, or internet filter utilized, operated or otherwise deployed by the Customer or any third party, including but not limited to, any government agency, regulatory body or statutory body; (v) necessary risk mitigation actions undertaken in response to external threats (such as DDOS attack attempts); (vi) use of the SaaS Product in violation of the SaaS Terms or Documentation; (vii) CyberArk’s suspension and/or termination of Customer’s right to use the SaaS Product in accordance with the SaaS Terms; or (viii) any Service Maintenance (collectively, “SLA Exclusions”). As used herein, “Service Maintenance” means

(i) routine weekly maintenance performed by CyberArk on Sundays during 3:30am-6:00am Eastern Time (EST or EDT, as appropriate) and for any Customer whose tenant is hosted on a data center located in the Asia-Pacific & Japan region, also from Sunday 10:00pm to Monday 12:30am SGT; (ii) other system upgrades and enhancements performed if announced in product, on the SaaS Product’s status page, the Service customer portal or via email, at least two days in advance; or (iii) emergency maintenance outside of the routine or pre-scheduled maintenance window that is reasonably required to apply patches or fixes, or to undertake other urgent maintenance activities. CyberArk will make reasonable efforts to limit the Service Maintenance window to the minimum possible to avoid disruption to the Service.

Annex 1

Uptime Percentage per SaaS Product

SaaS Product - Uptime Percentage

All SaaS Products available as of the date hereof, except as specifically mentioned in this table- 99.9%

Privilege Cloud - 99.95%

Remote Access - 99.95%

Dynamic Privilege Access - 99.95%

Endpoint Privilege Manager - 99.95%

Cloud Entitlements Manager - 99.95%

Secure Cloud Access - 99.95%

Identity - 99.99%

SAAS SUBSCRIPTION AND SERVICES AGREEMENT

Due to the document exceeding the allotted character limits, the full documentation can be located at "SaaS-and-Services-Agmt--CYBR-Global--20240517". We have included what we can below.

This SAAS SUBSCRIPTION AND SERVICES AGREEMENT ("Agreement") is made as of the later signing date below (“Effective Date”) by and between CyberArk and ____________ incorporated and registered in __________ and having a place of business at _____________ ("Customer"), each a “Party” and both the “Parties.” Capitalized terms used herein are defined in the “Definitions and Interpretation” section of this Agreement.

Background: Customer wishes to purchase certain SaaS Products and Professional Services as stated in the applicable Order or SOW entered into by the Parties pursuant to the terms of this Agreement. In consideration of their mutual promises and other good and valuable consideration, the Parties agree as follows:

1. Access and Use

1.1. Access and Use. CyberArk grants Customer, during the Subscription Term, a non-exclusive, non-transferable right to access and use (and permit Authorized Users of Customer and its Affiliates to access and use) the SaaS Products and applicable Documentation solely for Customer’s and its Affiliates’ internal business purposes in accordance with the Documentation and in the quantity specified in the applicable Order. Such license grant is subject to payment of all applicable fees set forth in the Order or payment in accordance with an Indirect Order through a Channel Partner (as appropriate) and the terms and conditions of this Agreement. CyberArk may update or upgrade the SaaS Products from time-to-time.

1.2. Access and Use Restrictions. Customer shall not (directly or indirectly): (a) copy or reproduce the SaaS Products or the Documentation except as permitted under this Agreement; (b) exceed the subscribed quantities, Authorized users or other entitlement measures of the SaaS Products as set forth in the applicable Order; (c) remove or destroy any copyright, trademark or other proprietary marking or legends placed on or contained in the SaaS Products, Documentation or CyberArk Intellectual Property; (d) assign, sell, sublicense, distribute or otherwise transfer or make available the rights granted to Customer under this Agreement to any third party except as expressly set forth herein; (e) modify, reverse engineer or disassemble the SaaS Products; (f) except to the limited extent applicable laws specifically prohibit such restriction, decompile, attempt to derive the source code or underlying ideas or algorithms of any part of the SaaS Products, attempt to recreate the SaaS Products or use the SaaS Products for any competitive or benchmark purposes; (g) create, translate or otherwise prepare derivative works based upon the SaaS Products, Documentation or CyberArk Intellectual Property; (h) interfere with or disrupt the integrity or performance of the SaaS Products; (i) attempt to gain unauthorized access to the SaaS Products or its related systems or networks, or perform unauthorized penetrating testing on the SaaS Products; (j) use the SaaS Products in a manner that infringes on the Intellectual Property rights, publicity rights, or privacy rights of any third party, or to store or transfer defamatory, trade libelous or otherwise unlawful data; or (k) except as otherwise agreed by the Parties in the applicable BAA, store in or process with the SaaS Products any personal health data, credit card data, personal financial data or other such sensitive regulated data not required by the Documentation, or any Customer Data that is subject to the International Traffic in Arms Regulations maintained by the United States Department of State. Fees for the SaaS Products are based on use of the SaaS Products in a manner consistent with the

Documentation. If Customer uses, or is reasonably suspected of using, the SaaS Products in violation of the Documentation or exceeding the licensed quantities or other entitlement measures as set forth in an applicable Order, Customer shall cooperate with CyberArk to resolve any non-compliance, which may include payment for any such overages at then-current applicable rates.

1.3. Login Access to the SaaS Products. Customer is solely responsible for ensuring: (i) that only appropriate Authorized Users have access to the SaaS Products; (ii) that such Authorized Users have been trained in proper use of the SaaS Products; and (iii) proper usage of passwords, tokens and access procedures with respect to logging into the SaaS Products. CyberArk may refuse registration of or suspend Customer's or a specific user's access and use of the SaaS Products if CyberArk knows or reasonably suspects that Customer's access or use is malicious or otherwise harmful to the Customer itself, the SaaS Products or CyberArk's other customers. CyberArk will provide notice prior to such suspension if permitted by applicable law and unless CyberArk reasonably believes that providing such notice poses a risk to the security of the SaaS Products. CyberArk will promptly reinstate Customer's access and use once the issue has been resolved.

1.4. Professional Services License. Subject to full and final payment for Professional Services (either directly or in accordance with section 2.3 "Indirect Orders") and the terms of this Agreement, CyberArk grants Customer a non-exclusive, non-transferable, non-assignable license to use (and to permit its Authorized Users to use) solely for Customer's and its Affiliates' internal use any Intellectual Property provided by CyberArk to Customer as a result of, or otherwise incorporated into, the Professional Services (excluding the SaaS Products).

1.5. Third Party Materials. The SaaS Products include Third-Party Materials, use of which is subject to their respective OSS Licenses as indicated in the Documentation. CyberArk warrants that the inclusion of such Third-Party Materials in the SaaS Products will not prevent Customer from exercising the license rights provided to Customer herein in respect of the SaaS Products or limit Customer's ability to use the SaaS Products in accordance with the Documentation. Nothing herein shall derogate from mandatory rights Customer may have under any OSS Licenses, if any. Customer may obtain a copy of the source code for certain Third-Party Materials by following the instructions set forth in the Documentation.

1.6. Support. As part of its provision of the SaaS Products, CyberArk shall make available technical support to Customer in accordance with the Support Services terms applicable to the SaaS Products. Upon notification from CyberArk, Customer shall promptly; update any Agents on Customer systems that interact with the SaaS Products; and/or as applicable, ensure that all Authorized Users download and install all available updates for locally installed components without undue delay. Customer acknowledges and agrees that its failure to timely install such updates may result in disruptions to or failures of the SaaS Products, security risks or suspension of Customer's access to the SaaS Products, without any liability on the part of CyberArk to Customer.

1.7. SaaS Product Usage Analytics. CyberArk and its Affiliates shall be permitted to collect and use Usage Analytics for its reasonable business purposes and for Customer's benefit (including research and development, statistical analyses, monitoring and management of CyberArk's products). Other than for the purpose of providing the SaaS Products to Customer, in the event CyberArk discloses Usage Analytics or any part thereof to third parties (either during the Subscription Term or thereafter) such data shall be deidentified so that it will not identify Customer or its Authorized Users. The foregoing shall not limit in any way CyberArk's confidentiality obligations pursuant to section 4 below.

2. Payment and Taxes

2.1. Payment Terms. Without prejudice to Customer's rights set out elsewhere in this Agreement, all SaaS Products fees are non-refundable and payable in advance. CyberArk may invoice: (a) for purchases of SaaS Products, upon delivery; and (b) for Professional Services (if applicable), according to the nature of the Professional Services: (i) upon CyberArk's receipt of the applicable Order for the Professional Services; (ii) monthly as rendered; or (iii) as otherwise set forth in the applicable Order or SOW. Where:

(A) Customer is paying CyberArk directly, Customer shall pay all invoices within thirty (30) days of date of invoice, without any deduction or set-off (except for any amount disputed promptly and in writing by Customer in good faith), and payment will be sent to the address specified by CyberArk. Any amounts arising in relation to this Agreement not paid when due will be subject to a late charge of one and one-half percent (1 ½ %) per month on the unpaid balance or the maximum rate allowed by law, whichever is less; or

(B) Customer places an Indirect Order, CyberArk grants the rights described in this Agreement in consideration for and subject to: (a) Customer's agreement to comply with the pricing and payment terms of the Indirect Order, to be separately agreed between Customer and the applicable Channel Partner; and (b) Customer's agreement to comply with its obligations set forth in this Agreement (including the restrictions on use of the SaaS Products).

Notwithstanding the foregoing, the final sales price or rate shall be freely and independently determined between the applicable Channel Partner and Customer. For the avoidance of doubt, in the case of such an Indirect Order, any indication in this Agreement of an agreement between Customer and CyberArk for the price payable by Customer for such Indirect Order shall be null and void and not form a binding part of this Agreement and the provisions of this Agreement related to payment terms, pricing and/or order procedures shall not apply.

2.2. Taxes. The fees and charges covered by this Agreement are exclusive of any Indirect Taxes imposed or levied, currently or in the future based on applicable legislation, on the SaaS

Products and Professional Services. Unless otherwise agreed between the Parties, Customer will be liable for compliance with reporting and payment of such Indirect Taxes in its tax jurisdiction. CyberArk shall include the Indirect Taxes on its invoice to Customer and remit such Indirect Taxes collected to the relevant authority if required by applicable law. For the avoidance of doubt, CyberArk will be responsible for direct taxes imposed on CyberArk's net income or gross receipts in its tax jurisdiction. Notwithstanding the forgoing, all payments made under this Agreement shall be in cleared funds, without any deduction or set-off, and free and clear of and without deduction from any Indirect Taxes or other withholdings of any nature.

3. Rights in Intellectual Property

3.1. Intellectual Property. Except for the rights granted in this Agreement, all rights, title, and interest in and to the SaaS Products, Documentation, and CyberArk Intellectual Property are hereby reserved by CyberArk, its Affiliates or licensors. Except as provided for herein, all rights, title, and interest in and to Customer Intellectual Property are hereby reserved by Customer, its Affiliates or licensors. Nothing in this Agreement shall transfer ownership of any Intellectual Property rights from one Party to the other. Customer shall not prohibit or enjoin CyberArk at any time from utilizing any skills or knowledge of a general nature acquired during the course of providing Professional Services, including using information publicly known or made available or that could reasonably be acquired in similar work performed for another customer of CyberArk.

3.2. Customer Data. Customer owns all right, title and interest in all Customer Data. Nothing in this Agreement shall be construed to grant CyberArk any rights in Customer Data beyond those expressly provided herein. Customer grants CyberArk and its Affiliates the limited, non-exclusive, worldwide license to view and use the Customer Data for the purpose of providing and improving the SaaS Products.

3.3. Suggestions. To the extent that Customer provides CyberArk with Suggestions, such Suggestions shall be free from any confidentiality restrictions that might otherwise be imposed upon CyberArk pursuant to this Agreement, and may be implemented by CyberArk in its sole discretion. Customer acknowledges that any CyberArk products or materials incorporating any such Suggestions shall be the sole and exclusive property of CyberArk.

3.4. AI Features. Certain features within the SaaS products use algorithmic analysis, artificial intelligence and/or machine learning technologies (“AI Features”). Use of the AI Features is subject to the Documentation and CyberArk's Responsible AI Policy found at https://www.cyberark.com/trust/responsible-ai/. Information regarding opting-out of AI Features is located in the Documentation.

4. Confidentiality

4.1. Confidential Information. The Parties acknowledge that each may disclose certain valuable confidential and proprietary information to the other Party. The receiving Party may only use the disclosing Party's Confidential Information to fulfil the purposes of this Agreement and in accordance with the terms of this Agreement. The receiving Party will protect the disclosing Party's Confidential Information by using at least the same degree of care as the receiving Party uses to protect its own Confidential Information of a like nature (but no less than a reasonable degree of care) to prevent the unauthorized use, dissemination, disclosure or publication of such Confidential Information. Notwithstanding the foregoing, the receiving Party may disclose Confidential Information to its (and its Affiliates) employees, advisors, consultants and agents on a need-to-know basis and provided that such party is bound by obligations of confidentiality substantially similar to those contained herein. This section 4 supersedes any and all prior or contemporaneous understandings and agreements, whether written or oral, between the Parties with respect to Confidential Information and is a complete and exclusive statement thereof. Additionally, the obligations set forth in section 5.4 and not this section 4 herein apply to Customer Data.

4.2. Exceptions. Information will not be deemed Confidential Information if it: (i) is known to the receiving Party prior to receipt from the disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (ii) becomes known (independently of disclosure by the disclosing Party) to the receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (iii) becomes publicly known or otherwise ceases to be secret or confidential, except through a breach of this Agreement by the receiving Party; or (iv) is independently developed by the receiving Party without use of or reliance upon the disclosing Party's Confidential Information and the receiving Party can provide evidence to that effect. The receiving Party may disclose Confidential Information pursuant to the requirements of a court, governmental agency or by operation of law but shall (to the extent permissible by law) limit such disclosure to only the information requested and give the disclosing Party prior written notice sufficient to permit the disclosing Party to contest such disclosure.

4.3. Advertising and Publicity. Neither Party shall make or permit to be made any public announcement concerning the existence, subject matter or terms of this Agreement or the relationship between the Parties without the prior written consent of the other Party except as expressly permitted in this section. Customer grants CyberArk and its Affiliates during the term of the Agreement the right to use Customer's trade names, logos, and symbols ("Customer Marks") in its public promotional materials and communications for the sole purpose of identifying Customer as a CyberArk customer. CyberArk shall not modify the Customer Marks, or display the Customer Marks any larger or more prominent on its promotional materials than the names, logos, or symbols of other CyberArk customers. The foregoing promotional materials and communications may be created, displayed, and reproduced without Customer's review, provided that they are in compliance with this section and any Customer Marks usage guidelines provided by Customer to CyberArk in writing.

5. Security and Processing of Personal Data

5.1. Customer Data Content. As between CyberArk and Customer, Customer is solely responsible for: (i) the content, quality and accuracy of Customer Data as made available by Customer and by Authorized Users; (ii) providing notice to Authorized Users with regards to how Customer Data will be collected and used for the purpose of the SaaS Products; (iii) ensuring Customer has a valid legal basis for processing Customer Data and for sharing Customer Data with CyberArk (to the extent applicable); and (iv) ensuring that the Customer Data as made available by Customer complies with applicable laws and regulations including (where applicable) Applicable Data Protection Laws.

5.2. Data Protection Laws. The Parties shall comply with their respective obligations under the Applicable Data Protection Laws. In particular, if Customer is established in the European Economic Area ("EEA"), in Switzerland, in the United Kingdom ("UK") or in California, or will, in connection with the SaaS Products, provide CyberArk with personal data relating to an individual located within the EEA, Switzerland the UK or California, the Parties shall comply with the Data Processing Addendum found at https://www.cyberark.com/CyberArk-Data-Processing-Addendum.pdf ("DPA") which in such case is hereby incorporated into this Agreement.

5.3. HIPAA (Health Insurance Portability and Accountability Act). To the extent that (a) Customer is established in the United States; and (b) is a "covered entity" or a "business associate" and includes "Protected Health Information" (as these terms are defined in the Business Associate Agreement ("BAA")) in Customer Data, the Parties shall comply with the BAA found at https://www.cyberark.com/lgl/CyberArk-BAA.pdf. In such case, the terms of the BAA are hereby incorporated into this Agreement by reference.

5.4. Security of Customer Data. CyberArk shall: (i) ensure that is has in place appropriate administrative, physical and technical measures designed to protect the security and confidentiality of Customer Data against any accidental or illicit destruction, alteration or unauthorized access or disclosure to third parties; and (ii) access and use the Customer Data solely to perform its obligations in accordance with the terms of this Agreement, and as otherwise expressly permitted in this Agreement. CyberArk shall not materially diminish its security controls with respect to Customer Data during a particular SaaS Products term. The obligations set forth in this Section 5.4 are in addition to any confidentiality, privacy, security or other requirements contained in the BAA or DPA, as applicable.

5.5. Bring Your Own Key. If Customer chooses to enable the "Bring Your Own Key" functionality for data encryption made available by CyberArk for certain SaaS Products ("BYOK"), Customer acknowledges that (i) Customer shall bear sole responsibility for the hosting, use, protection, rotation and management of such encryption key and any loss, damage, unavailability or non-performance resulting therefrom; (ii) Customer shall provide CyberArk with access to the encryption key at all times in order to encrypt Customer Data and proper performance of the SaaS Products; and (iii) CyberArk has no control over the encryption key and specifically is unable to de-encrypt, restore, recover or otherwise retrieve Customer Data in the event the encryption key is lost, damaged or otherwise not made available to CyberArk. If BYOK functionality is enabled by Customer, CyberArk disclaims any and all responsibility and liability for unavailability or non-performance of the SaaS Products caused by loss, damage or any unavailability of the encryption key.

6. Warranties

6.1. Limited SaaS Products Warranty. During the applicable Subscription Term, CyberArk warrants that: (a) the SaaS Products will perform in substantial conformity with the Documentation, and (b) CyberArk will use industry standard measures designed to detect viruses, worms, Trojan horses or other unintended malicious or destructive code in the SaaS Products. The foregoing warranties are void if the failure of the SaaS Products has resulted from negligence, error, or misuse of the SaaS Products (including use not in accordance with the Documentation) by Customer, the Authorized User or by anyone other than CyberArk. Customer shall be required to report any breach of warranty to CyberArk within a period of thirty (30) days of the date on which the incident giving rise to the claim occurred. CyberArk's sole and exclusive liability, and Customer's sole and exclusive remedy, for breach of these warranties will be for CyberArk, at its expense, to use reasonable commercial efforts to correct such nonconformity within thirty (30) days of the date that notice of the breach was provided; and, if CyberArk fails to correct the breach within such cure period, Customer may terminate the affected Order and, in such event, CyberArk shall provide Customer with a pro-rata refund of any unused pre-paid fees paid for the period following termination as calculated on a monthly basis for the affected SaaS Products. Without derogating from CyberArk's obligations under this Agreement, Customer warrants that it shall take and maintain appropriate steps within its control to protect the confidentiality, integrity, and security of its Confidential Information and Customer Data, including: (i) operating the SaaS Products in accordance with the Documentation and applicable law and; and (ii) dedicating reasonably adequate personnel and resources to implement and maintain the security controls set forth in the Documentation. Customer will be responsible for the acts and omissions of its Authorized Users.

6.2. Professional Services Warranty. CyberArk warrants that: (a) it is competent and possesses the necessary expertise and financial resources to perform the Professional Services; (b) the Professional Services will be performed in a professional and workmanlike manner, consistent with reasonably applicable industry standards; and (c) all personnel performing Professional Services shall have suitable training, education, experience, know-how and skill to perform the relevant Professional Services in a competent manner. Customer shall notify CyberArk in writing of any claims under the foregoing Professional Services warranties within five (5) business days following CyberArk's performance of the defective Professional Services.

6.3. Compliance with Law. Each Party shall comply with all applicable, laws and regulations in connection with the performance of its obligations and the exercise of its rights under this Agreement.

6.4. Disclaimer. Any and all warranties, expressed, incorporated or implied are limited to the extent and period mentioned in this Agreement. To the maximum extent allowed by applicable law, CyberArk disclaims (and disclaims on behalf of its licensors and/or contributors to any Third-Party Materials) all other warranties, conditions and other terms, whether express or implied or incorporated into this Agreement by statute, common law or otherwise, including the implied conditions and warranties of merchantability and fitness for a particular purpose. CyberArk will have no responsibility or liability for delays, failures or losses (i) attributable or related in any way to the use or implementation of third-party hardware, software or services not provided by CyberArk; or (ii) use of the SaaS Products not in accordance with the Documentation.

7. Indemnification

7.1. Infringement Indemnity. CyberArk shall defend and indemnify Customer and/or its Affiliates and their officers, directors and employees against all third-party claims, suits and proceedings and all directly related losses, liabilities, damages, costs and expenses (including reasonable attorneys' fees) resulting from the violation, misappropriation, or infringement of such third party's patent, copyright, trademark or trade secret caused by Customer's use of the SaaS Products in accordance with this Agreement and the Documentation.

7.2. Customer Data and Use Indemnity. Customer shall defend and indemnify CyberArk and/or its Affiliates and their officers, directors and employees against any third-party claims, suits and proceedings (including those brought by a government entity), and all directly related losses, liabilities, damages, costs and expenses (including reasonable attorneys' fees), resulting from: (i) an alleged infringement or violation by the Customer Data of such third-party's patent, copyright, trademark, trade secret; or (ii) CyberArk's use of the Customer Data violating applicable law, provided that such use is in accordance with the terms of this Agreement and (where applicable) with the terms of the DPA and/ or the BAA.

7.3. Process. Each Party's defense and indemnification obligations herein will become effective upon, and are subject to: (a) the indemnified Party's prompt notification to the indemnifying Party of any claims in writing; and (b) the indemnified Party providing the indemnifying Party with full and complete control, authority and information for the defense of the claim, provided that the indemnifying Party will have no authority to enter into any settlement or admission of the indemnified Party's wrongdoing on behalf of the indemnified Party without the indemnified Party's prior written consent (not to be unreasonably withheld). At the indemnifying Party's request, the indemnified Party shall reasonably cooperate with the indemnifying Party in defending or settling any claim.

7.4. Exclusions. The above CyberArk obligations to defend and indemnify will not apply in the event that a claim arises from or relates to: (a) use of the SaaS Products not in accordance with the Documentation and this Agreement; (b) use of the SaaS Products in violation of applicable laws; (c) any modification, alteration or conversion of the SaaS Products not created or approved in writing by CyberArk; (d) any combination of the SaaS Products with any computer, hardware, software, data or service not provided by CyberArk; (e) CyberArk's compliance with specifications, requirements or requests of Customer; or (f) Customer's gross negligence or willful misconduct.

7.5. Remedies. If a SaaS Product becomes, or CyberArk reasonably determines that a SaaS Product is likely to become, subject to a claim of infringement for which CyberArk must indemnify Customer as described above, CyberArk may at its option and expense: (a) procure for Customer the right to continue to access and use that SaaS Product; (b) replace or modify that SaaS Product so that it becomes non-infringing without causing a material adverse effect on the functionality provided by that SaaS Product; or (c) if neither of the foregoing options are available in a timely manner on commercially reasonable terms, terminate the affected Order and provide Customer with a pro-rata refund of any unused pre-paid fees paid for the period following termination as calculated on a monthly basis for that SaaS Product. This section titled "Indemnification" states the sole liability of CyberArk and the exclusive remedy of Customer with respect to any indemnification claims arising out of or related to this Agreement.

8. Limitation of Liability

8.1. Maximum Liability. Except for liability caused by CyberArk's intellectual property infringement indemnification obligations in section 7.1, Customer's data infringement indemnity in section 7.2, or Customer's payment obligations herein, in no event will either Party's maximum aggregate liability arising out of or related to this Agreement, regardless of the cause of action and whether in contract, tort (including negligence), warranty, indemnity or any other legal theory, exceed the total amount paid or payable to CyberArk under this Agreement during the twelve (12) month period preceding the date of initial claim.

8.2. No Consequential Damages. Neither Party will have any liability to the other Party for any loss of profits or revenues, loss of goodwill, or for any indirect, special, incidental, consequential or punitive damages arising out of, or in connection with this Agreement, however caused, whether in contract, tort (including negligence), warranty, indemnity or any other legal theory, and whether or not the Party has been advised of the possibility of such damages.

8.3. Construction. This Agreement is not intended to and will not be construed as excluding or limiting any liability which cannot be limited or excluded by applicable law, including liability for: (a) death or bodily injury caused by a Party's negligence; or (b) gross negligence, willful misconduct, or fraud.

9. Restricted Rights and Export Control

9.1. Export Control. The exportation of the SaaS Products and Documentation, and all related technology and information thereof are subject to U.S. laws and regulations pertaining to export controls and trade and economic sanctions, including the U.S. Export Administration Act, Export Administration Regulations, the Export Control Reform Act, and the Office of Foreign Assets Control's sanctions programs, the laws of the State of Israel, and the laws of any country or organization of nations within whose jurisdiction Customer (or its Authorized Users who may use or otherwise receive the SaaS Products as expressly authorized by this Agreement) operates or does business, as amended, and the rules and regulations promulgated from time to time thereunder. Specifically, Customer hereby undertakes not to export, re-export, access or grant access to the SaaS Products and all related technology, information, materials and any upgrades thereto to: (a) any Prohibited Persons; (b) any country to which such export, re-export or access from is restricted or prohibited per the foregoing applicable laws; or (c) otherwise in violation of any applicable export or import restrictions, laws or regulations. Customer also certifies that it is not a Prohibited Person nor owned, controlled by, or acting on behalf of a Prohibited Person.

9.2. Commercial Computer Software and FedRAMP Products. If Customer is an agency or contractor of the United States Government, Customer acknowledges and agrees that: (i) the SaaS Products (including any software forming a part thereof) were developed entirely at private expense; (ii) the SaaS Products (including any software forming a part thereof) in all respects constitute proprietary data belonging solely to CyberArk; (iii) the SaaS Products (including any software forming a part thereof) are not in the public domain; and (iv) the software forming a part of the SaaS Products is “Commercial Computer Software” as defined in sub-paragraph (a)(1) of DFARS section 252.227-7014 or FAR Part 12.212. Customer shall provide no rights in the Software (including any software forming a part thereof) to any U.S. Government agency or any other party except as expressly provided in this Agreement. If Customer places an Order for SaaS Products which are designated as “FedRAMP Authorized,” the CyberArk Rider to SaaS Terms of Service for FedRAMP Products found at https://www.cyberark.com/contract-terms/ is incorporated herein and will apply to CyberArk’s provision of such SaaS Products.

10. Professional Services. If Customer purchases Professional Services, this section titled “Professional Services” will apply. In the event of a conflict between any provisions of the Agreement and a SOW, the provisions of the SOW will govern with respect to the specific Professional Services described therein.

10.1. Performance; Personnel. CyberArk will perform the Professional Services on a time and materials and non-exclusive basis, or as otherwise detailed in the relevant Order or SOW, and as more particularly detailed in the relevant SOW. Customer will provide reasonable support, services, material, facilities and other items…

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

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.

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

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 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.

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.

Any Applicable SLA Goes Here

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

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

Respondent Name: Hayes e-Government Resources

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:

Service Level Agreement for Hosted Services This Service Level Agreement ("SLA") between Tenable ("Tenable") and Customer is subject to the applicable license or subscription agreement between Tenable and Customer under which the Customer licenses the Hosted Services, or if the parties have not executed such separate agreement, the Tenable Master Agreement located at http://static.tenable.com/prod_docs/tenable_slas.html (the "Agreement"). All defined terms used in this SLA and not defined herein shall have the meaning assigned to them in the Agreement. Tenable shall provide the Hosted Services and Software in connection with the Agreement. This SLA governs Tenable's performance and delivery of the Hosted Services to Customer.

1. Definitions.

"Potential Uptime" means the amount of time in a given month. "Production Uptime" represents the amount of time in a given month that Customer has the ability to log in or access the Hosted Services user interface (or authenticate to APIs) and perform associated Scanning related activity. Potential Uptime is measured by Tenable in a given month by the following calculation: Production Uptime = (Potential Uptime – Hosted Services Interruption Time) / (Potential Uptime – Exclusions) "Hosted Services Interruption Time" is the period of time for which the Hosted Services (or any material portion thereof) are unavailable due to issues caused by or attributable to Tenable or its agents. Hosted Services Interruption Time does not include Regular Maintenance or Scheduled Maintenance. "Regular Maintenance" is the period of time under which the Hosted Services may be unavailable for recurring maintenance work. Tenable attempts to schedule this time when usage of the Hosted Services is light across Tenable's customer base and therefore, Tenable shall use commercially reasonable efforts to only conduct Regular Maintenance daily between the hours of 7AM and 9AM (ET) and non-business days. Regular Maintenance is required in order to update Tenable's plug-in databases as well as to maintain system health requirements. Tenable shall use commercially reasonable efforts to minimize any Regular Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Regular Maintenance. "Scheduled Maintenance" is the period of time under which the Hosted Services may be unavailable for non-recurring maintenance. Scheduled Maintenance is required in order to provide updates to the Hosted Services as well as to maintain system health requirements. Tenable shall provide Customer at least twelve (12) hours advance notice prior to Scheduled Maintenance; provided, however, Tenable shall endeavor to provide at least twenty-four (24) hours advanced notice for Scheduled Maintenance. Notice for Scheduled Maintenance will be provided at the following URL or successor location: status.tenable.com. Tenable shall use commercially reasonable efforts to minimize any Scheduled Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Scheduled Maintenance. "Emergency Maintenance" describes maintenance for certain emergency situations, where

advance notice may be not be feasible, possible or practical. Tenable shall use commercially reasonable efforts to minimize any Emergency Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Periods of Emergency Maintenance shall be included in Hosted Services Interruption Time. Tenable Confidential and Proprietary SLA v.3

2. Service Levels Commitment. Tenable commits to provide a 99.95% Production Uptime with respect to the Hosted Services during each calendar month of the subscription term.

3. Service Level Credits. If Tenable fails to perform the Hosted Services in accordance with the Service Level Commitment, then Customer may request a Service Level Credit in accordance with this SLA. Service Level Credits shall be Customer's sole and exclusive remedy for unavailability or performance degradation of the specific Hosted Services.

4. Weighting Factor. The "Weighting Factor" for calculation of the Service Level Credit is set forth below and correlates to the relative unavailability of the Hosted Service in a given month.

Production Uptime between 99.95% and 100% = 0 Production Uptime between 95.00% and 99.94% = .1 Production Uptime between 90.00% and 94.99% = .15 Production Uptime below 90% = .2

5. Calculation of Service Level Credits. The following equation shall be used to calculate any Service Level Credits: Service Level Credit (in $) = Weighting Factor multiplied by the monthly fee for applicable Hosted Service.

Example: Production Uptime in a given month is 95%. The monthly fee for the Hosted Service is $100 (Annual fee for the Hosted Services is $1,200). Service Level Credit (in $) = (0.1) x $100 = $10.

If Customer has paid in advance for one or more years of the Hosted Services, monthly fees will be calculated on a pro rata basis.

6. Exclusions. "Exclusions" shall mean any time for which the Hosted Services are unavailable to do any of the following: (i) Customer's breach of, or failure to perform any obligations under, this SLA or the Agreement; (ii) issues relating to Customer's environment, internal networks, computer systems, firewalls or Customer's inability to connect to the internet; (iii) Force Majeure Events; or (iv) issues arising from failures, acts or omissions Tenable's upstream service providers (i.e. AWS).

7. Requests. In order to receive a Service Level Credit, Customer must request such by emailing Tenable at credits@tenable.com, within 10 days of the end of the applicable month. If Customer is past due or in default with respect to any payment or any material contractual obligations to Tenable, Customer is not eligible for any Service Level Credit. Service Level Credits are non-refundable and may only be applied to future upgrades or renewals of the specific Tenable Hosted Services affected.

8. Changes. This Service Level Commitment may be amended by Tenable in its reasonable discretion but only after providing thirty (30) days' advance notice. Tenable may provide such notice either as a note on the screen presented upon logging in to the Hosted Services, by posting updated terms on Tenable's website, or by email to the email addressed registered with Customer's account. This SLA was updated on October, 2023 (ver 3).

Master Agreement, accepted via a click-thru acknowledgement at time of installation:

Due to the document exceeding the allotted character limit, the full documentation can be located at https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf . We have included what we can below.

TENABLE MASTER AGREEMENT This Master Agreement (this “Agreement”) is made by and between Tenable (as defined below) and the customer licensing Products and/or receiving services (“Customer”) with an effective date as of the date Customer clicks to accept this Agreement (the “Effective Date”). Hereinafter, each of Tenable and Customer may be referred to collectively as the “Parties” or individually as a “Party”.

1. Definitions. (a) “Affiliate” means any entity that controls, is controlled by, or is under common control with a Party. “Control” shall mean: (1) ownership (either directly or indirectly) of greater than fifty percent (50%) of the voting equity or other controlling equity of another entity; or (2) power of one entity to direct the management or policies of another entity, by contract or otherwise. (b) “Documentation” means the then-current official user manuals and/or documentation for the Products available at docs.tenable.com (or a successor location). (c) “Hosted Services” are a type of service offered through Tenable’s cloud-based software as a service (SaaS) platform and include Scans and access to and use of the hosted environment (the “Hosted Environment”). (d) “Product(s)” means any of the products that Tenable offers, including Software, Hosted Services, Hardware (if any), Support Services and Professional Services. (e) “Professional Services” means services purchased, including consulting services which are relevant to the implementation and configurations of Tenable Products as well as on-site or virtual training courses. Generally, Professional Services are defined either in a separate SOW or a Services Brief. Professional Services do not include the Hosted Services or Support Services. (f) “Scan(s)” are a function performed by the Software and/or the Hosted Services on Scan Targets, which are conducted in order to provide data to Customer regarding its network security. “PCI Scans” are a specific type of Scan designed to assess compliance with the Payment Card Industry Data Security Standard. “Scan Data” is the resulting information created by the Scan. “Scan Target(s)” are the targets or subjects of a Scan. (g) “Services Brief” means the document which outlines Tenable’s basic, pre-packaged installation or training Professional Services offered under a Tenable SKU and which do not require a separate SOW. Current versions of Services Briefs may be found at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). For the avoidance of doubt, Customer may purchase commercial off the shelf SKU-based Professional Services without executing a separate Statement of Work. A “SOW” or “Statement of Work” shall further describe Professional Services, the terms of which may be customized and which shall require execution by the Customer. (h) “Software” means each software product made available by Tenable under this Agreement for download. Software includes patches, updates, improvements, additions, enhancements and other modifications or revised versions of the same that may be provided to Customer by Tenable from time to time. (i) “Technical Data” means data Customer uploads or runs through or on the Products, or is otherwise generated thereby, including information regarding licensing metrics and product behavioral data. (j) “Tenable” means: (i) Tenable, Inc., if Customer is a commercial entity or individual located in North or South America (Tenable, Inc. is a Delaware corporation having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); (ii) Tenable 2 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 Public Sector LLC, if Customer is an agency or instrumentality of the United States Government, a commercial entity operating predominantly as a federal systems integrator

for eventual sale or resale or for the benefit of the United States Government, or an agency or instrumentality of a State or local government within the United States (Tenable Public Sector LLC is a Delaware limited liability company having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); or (iii) Tenable Network Security Ireland Limited, if Customer is located outside of North or South America (Tenable Network Security Ireland Limited is a private limited company having offices at 81b Campshires, Sir John Rogerson's Quay, Dublin 2, Ireland).

2. Orders and Transactions. (a) Reseller Transactions. If Customer purchases Tenable Products through an authorized Tenable reseller (a "Reseller"), all terms related to pricing, billing, invoicing and payment ("Payment Terms") set forth in this Agreement (if any) shall not apply. For the avoidance of doubt, all such Payment Terms shall be as agreed to between Customer and Reseller. To place an order, Customer shall provide the Reseller with a purchase order (or other similar document acceptable to Reseller) in response to a valid quote from such Reseller. Following Reseller's receipt of such purchase order, Tenable shall issue a sales order confirmation or other similar order acceptance document (the "Ordering Document"). No order shall be deemed accepted by Tenable until Tenable issues the Ordering Document. The Ordering Document shall set forth all Products (and corresponding licensing metrics) purchased by Customer. (b) Direct Transactions. If the Parties have agreed to transact directly, the following Payment Terms shall apply. Customer agrees to pay all amounts due as specified in a Tenable invoice. Fees for Hosted Services are charged for access to the Host Environment (as defined herein), not actual usage. Payment is due within thirty (30) days from the date of Tenable's invoice to Customer. Customer will pay directly or reimburse Tenable for any taxes (including, sales or excise taxes, value added taxes, gross receipt taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, imposed on or arising out of this Agreement. Notwithstanding the foregoing, Tenable will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. Customer agrees to pay Tenable without deducting any present or future taxes, withholdings or other charges except those deductions it is legally required to make. If Customer is legally required to make any deductions or withholding, Customer agrees to provide evidence of such withholding upon request. If a certificate of exemption or similar document or proceeding is necessary in order to exempt any transaction from a tax, Customer shall provide such certificate or document to Tenable. (c) Delivery and Installation. Delivery of Tenable Products ("Delivery") shall be deemed to occur on the date of availability for electronic download or electronic access. Tenable has no duty to provide installation services for Tenable Products unless installation services are purchased separately.

3. Term and Termination. (a) Agreement Term. This Agreement shall commence upon the Effective Date and continue until terminated in accordance with the terms set forth herein. (b) License Term and Renewals. The "License Term" is the term of the license or subscription for Products as set forth in the Ordering Document. If this Agreement has been signed by both Parties, then unless otherwise agreed to in writing, any License Term, including renewals, shall be governed by the terms set forth herein. If this Agreement has been accepted via shrinkwrap or click through, upon any renewal of the License Term, the terms then available at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location) will govern such renewal. Customer agrees that use of the Products at the time of such renewal will be deemed full and adequate acceptance of the updated terms. (c) Termination for Cause. Either Party may terminate this Agreement for cause if the other Party materially breaches this Agreement provided that such breaching Party has received written notice of such breach and failed to cure such breach within thirty (30) days. If this Agreement is terminated for cause by either Party, Customer

shall remove all copies of the Products from any Customer systems and cease to use any Software or Hosted Services purchased hereunder. Further, Customer shall certify to Tenable that it has returned or destroyed all copies of the Software. If this Agreement is terminated for cause by Tenable, Customer shall remain responsible for any outstanding payment obligations throughout the rest of the License Term. (d) Termination for Convenience. Customer may terminate this Agreement for any lawful reason upon ninety (90) days' prior written notice to Tenable. If Customer terminates for convenience, Customer shall not receive a refund and shall remain obligated to pay for Products for which it has previously entered into a transaction as well as any additional payment obligations agreed upon prior to the termination date.

4. Products. (a) Product-Specific Terms. Pursuant to this Agreement, Customer may receive the right to use various Products as further described in the attached schedules (each, a "Schedule"). Terms related to Customer's use of Software are described in Schedule A 3 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 (Software). Terms related to Customer's use of Hosted Services are described in Schedule B (Hosted Services). Terms related to the provision of Professional Services are described in Schedule C (Professional Services). For each Product, Customer will have the right to use the corresponding Documentation. (b) Licensing Model. Product licenses shall be in accordance with the terms of the applicable licensing model as set forth in the Documentation and/or the Ordering Document, which may include limitations on Scan Targets, compute, storage, resource utilization, License Term, the number of users, seats, licenses and/or types of modules licensed. Product licenses shall commence upon Delivery and shall be either perpetual or subscription in nature. Tenable shall use commercially reasonable efforts to meter resource utilization and assess likeness or uniqueness of Scan Targets within each Product/module licensed. If Customer exceeds the license restrictions, Customer must purchase an upgraded license to allow for all actual or additional usage, and Tenable or its Reseller may promptly invoice Customer for any such overages at a price not to exceed Tenable's then-current rates. Discrepancies in Scan Target or utilization count is the sole responsibility of the Customer to resolve. (c) Restrictions on Use. Customer shall not directly or indirectly: (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive, obtain or modify the source code of the Products; (ii) reproduce, modify, translate or create derivative works of all or any part of the Products; (iii) remove, alter or obscure any proprietary notice, labels, or marks on the Products; (iv) without Tenable's prior written consent, use the Products in a service bureau, application service provider or similar capacity; (v) without signing Tenable's Managed Security Services Provider Addendum, use the Products to provide any managed service to a third party; (vi) use the Products in order to create competitive analysis or a competitive product or service; (vii) copy any ideas, features, functions or graphics in the Product; or (viii) without Tenable's prior written consent, interfere with or disrupt performance of Hosted Services (e.g., perform penetration testing on Tenable systems). Customer may only use the Products to manage or gather information from Scan Targets owned or hosted by Customer or its Affiliates, or third parties for which Customer has received express authorization to Scan. (d) Intellectual Property in Products. This Agreement does not transfer to Customer any title to or any ownership right or interest in the Products. Any rights in the Products not expressly granted in this Agreement are reserved by Tenable. If Customer provides Tenable with any comments, suggestions, or other feedback regarding the Product, Customer hereby assigns to Tenable all right, title and interest in and to such feedback. For clarity, such feedback shall not contain Customer Confidential Information and shall not reference or identify Customer or its users. (e) Customer Requirements. In order to use the Products, Customer must meet or exceed the specifications found in the

Documentation. (f) Product Features. Customer agrees that purchase of any Product is not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Tenable regarding future functionality or features. Tenable reserves the right to withdraw features from future versions of the Products provided that: (i) the core functionality of the affected Product remains the same; or (ii) Customer is offered access to a product or service providing materially similar functionality as the functionality removed from the affected Product. The preceding remedies under this Section 4(f) are the sole remedies available if Tenable withdraws features from the Products. (g) Rights Granted to Tenable. Provided that Tenable shall not publicly disclose any Customer Confidential Information, Tenable may: (i) use Technical Data for reasonable business purposes, including Support Services, license validation, research and development, feature creation, and Product testing; (ii) include aggregated and anonymized Technical Data in public materials; and (iii) retain Technical Data which is anonymized after the termination of this Agreement. (h) Hardware. Any Hardware purchased under this Agreement (if any) will be subject to the terms and conditions of Schedule D located at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). (i) Temporary Limitation. If Tenable reasonably believes: (i) Customer's use of the Products places an unreasonable or disproportionate burden on the Products; (ii) Customer's use of the Products poses a risk or threat to the Products (including any systems supporting the Products), Tenable, or a third party; or (iii) Customer's usage exceeds the limitations of the license, then Tenable may temporarily limit Customer's access to or use of the Products or any specific feature therein. Tenable may also suspend or limit access to the Products if Customer fails to make any payments related to this Agreement. Tenable will, to the extent practical under the circumstances, use commercially reasonable efforts to provide Customer with prior written notice of any such limitation (email or in product messaging shall be sufficient). When commercially reasonable, Tenable shall promptly restore access once the Customer has remediated the issue. For the avoidance of doubt, Customer is responsible for all normal fees during any period for which usage or access is limited pursuant to this section. (j) Additional Details on Use Restrictions for Tenable Security Network Ireland Limited. The following shall only apply for transactions with Tenable Security Network Ireland Limited. Notwithstanding anything in Section 4(c), decompiling the Product is 4 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 permitted to the extent the laws of Customer's jurisdiction give Customer the right to do so to obtain information necessary to render the Products interoperable with other software; provided, however, that Customer must first request such information from Tenable and Tenable may, in its discretion, either provide such information to Customer or impose reasonable conditions, including a reasonable fee, on such use of the Products to ensure that its proprietary rights in the Product are protected.

5. Support. (a) Support Services. Tenable shall provide Customer with support services (the "Support Services") in accordance with Tenable's then-current Technical Support Plans (available at http://static.tenable.com/prod_docs/tenable_slas.html or a successor location) and consistent with Tenable's End of Life and End of Sale definitions contained therein. The Support Services include bug fixes, updates (including new vulnerability plug-ins), or enhancements that Tenable makes generally available to users of the Products. The Support Services also include the provision of new minor (Example: 1.1.x to 1.2.x, etc.) and major version releases of the Products (Example: 1.x to 2.x, etc.). (b) Support Fees. Standard Support Services for Products licensed for a finite License Term will be provided at no additional charge beyond the license fee for the duration of the License Term. Support Services for Products licensed on a perpetual basis must

be purchased separately in advance. In all cases, premium support may be purchased at an additional charge. If during the course of a perpetual license Customer terminates or fails to renew the Support Services, Customer may, at any time during the term of this Agreement, request that Tenable reinstate the Support Services provided that Customer pays for the lapsed Support Services in an amount equal to the total fees Customer would have paid for the Support Services between the time Customer's Support Services lapsed and the then-current date.

6. Confidentiality. (a) Definition. "Confidential Information" means information learned or disclosed by a Party under this Agreement that should reasonably be assumed to be confidential or proprietary, including the Products and the terms of this Agreement. Confidential Information will remain the property of the disclosing Party, and the receiving Party will not be deemed by virtue of this Agreement or any access to the Confidential Information to have acquired any right, title or interest in or to the Confidential Information. (b) Obligations. Each Party agrees to only use the Confidential Information in connection with this Agreement or a purchase hereunder. The receiving Party agrees to hold the disclosing Party's Confidential Information confidential using at least the same level of protection against unauthorized disclosure or use as the receiving Party normally uses to protect its own information of a similar character, but in no event less than a reasonable degree of care. Each Party may share Confidential Information with its Affiliates or authorized contractors in the performance of its duties under this Agreement; provided, however, that each Party shall be responsible to ensure that such Affiliate or authorized contractors are bound by obligations of confidentiality at least as stringent as those set forth in this Agreement. (c) Exclusions. Confidential Information shall not include information that: (i) is already known to the receiving Party free of any confidentiality obligation; (ii) is or becomes publicly known through no wrongful act of the receiving Party; (iii) is rightfully received by the receiving Party from a third party without any restriction or confidentiality; or (iv) is independently developed by the receiving Party without reference to the Confidential Information. Confidential Information does not include Scan Data that has been aggregated or anonymized so that it is not attributable to the disclosing Party. If Customer requests or performs scans on third party Scan Targets, and such third party inquires with Tenable about the scan, Tenable shall inform Customer and allow Customer to resolve any disputes with the third party. If Customer fails to contact the third party, Customer agrees that Tenable may provide Customer's business contact information to the owner of the Scan Targets as well as to relevant authorities, and such disclosure shall not be considered a breach of confidentiality. (d) Sensitive Information. The Parties agree that Customer's disclosure of sensitive, personal information (e.g., social security numbers, national identity card numbers, personal credit card information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and health care data) ("Sensitive Information") is not required for Tenable to perform its duties under this Agreement or sell any Products hereunder. If Customer inadvertently or unintentionally discloses any Sensitive Information to Tenable, Customer shall identify to Tenable that it has disclosed Sensitive Information and Tenable shall promptly return and/or destroy such Sensitive Information. (e) Legal Disclosures; Remedies. The receiving Party may disclose Confidential Information if required to do so by law provided the receiving Party shall promptly notify the disclosing Party so that the disclosing Party may seek any appropriate protective order and/or take any other action to prevent or limit such disclosure. If required hereunder, the receiving Party shall furnish only that portion of the Confidential Information disclosure of which is legally required. The receiving Party acknowledges and agrees that the breach of any term, covenant or provision of this Agreement may cause irreparable harm to the disclosing Party and, accordingly, upon the threatened or

actual breach by the receiving Party of any term, covenant or provision of this Agreement, the disclosing Party shall 5 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 be entitled to seek injunctive relief, together with any other remedy available at law or in equity. The receiving Party will notify the disclosing Party promptly of any unauthorized use or disclosure of the disclosing Party's Confidential Information.

7. Representations and Warranties; Disclaimer. (a) Warranty of Authority. The Parties hereby represent and warrant that they have the full power and authority to enter into this Agreement. (b) Products. Product warranties and associated warranty periods are set forth in the relevant Schedules. (c) Antivirus Warranty. Tenable represents it has taken commercially reasonable efforts to ensure that the Products, at the time of Delivery, are free from any known and undisclosed virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that would erase data or programming or otherwise cause the Products to become inoperable or incapable of being used in the manner for which it was designed or in accordance with the Documentation. (d) Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT AND TO THE GREATEST EXTENT PERMITTED BY LAW, TENABLE OFFERS ITS PRODUCTS “AS-IS” AND MAKES NO OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF TITLE, NON INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SECURITY, INTEGRATION, PERFORMANCE AND ACCURACY, AND ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. THE WARRANTIES SET FORTH IN THIS AGREEMENT ARE MADE TO CUSTOMER FOR CUSTOMER'S BENEFIT ONLY. CUSTOMER'S USE OF THE PRODUCTS IS AT CUSTOMER'S OWN RISK. CUSTOMER UNDERSTANDS THAT ASSESSING NETWORK SECURITY IS A COMPLEX PROCEDURE, AND TENABLE DOES NOT GUARANTEE THAT THE RESULTS OF THE PRODUCTS WILL BE ERROR-FREE OR PROVIDE A COMPLETE AND ACCURATE PICTURE OF CUSTOMER'S SECURITY FLAWS, AND CUSTOMER AGREES NOT TO RELY SOLELY ON SUCH PRODUCTS IN DEVELOPING ITS SECURITY STRATEGY. CUSTOMER ACKNOWLEDGES THAT THE PRODUCTS MAY RESULT IN LOSS OF SERVICE OR HAVE OTHER IMPACTS TO NETWORKS, ASSETS OR COMPUTERS (INCLUDING MODIFICATION OF SCAN TARGETS), AND CUSTOMER IS SOLELY RESPONSIBLE FOR ANY DAMAGES RELATING TO SUCH LOSS OR IMPACT.

8. Limitation of Liability. (a) Direct Damages. The cumulative liability of one Party to the other for all claims arising from or relating to the Products or this Agreement (including without limitation, any cause of action sounding in contract, tort or strict liability) shall be limited to proven direct damages in an amount not to exceed, in the aggregate, the fees paid by Customer for the Products over the twelve (12) months immediately prior to the event giving rise to the claim. (b) Indirect Damages. Neither Party shall be liable to the other for any indirect, incidental, special, punitive, consequential or exemplary damages regardless of the nature of the claim. This prohibition on indirect damages shall include, but not be limited to, claims based on lost profits, cost of delay, any failure of Delivery, business interruption, cost of lost or damaged data, or liabilities to any third parties even if such Party is advised of the possibility thereof. (c) Carve Outs. The liability caps set forth in Sections 8(a) and 8(b) shall not apply to damages resulting from: (i) personal injury or death; (ii) fraud or willful misconduct; (iii) indemnification obligations set forth in Section 9 (Indemnification); or (iv) Customer's breach of Section 4(c) (Restrictions on Use). (d) Limitations; Time Period. Each of the limitations set forth in this Section 8 shall be enforced to the

fullest extent of the law. Any laws preventing such limitations shall only apply to the extent required by law and the remaining unaffected terms shall apply in full. Unless expressly prohibited by law, each Party shall have a period of no greater than twelve (12) months from the date the cause of action accrues to bring a claim against the other Party for such cause of action.

9. Indemnification. (a) Indemnification Obligations. (i) By Tenable. Tenable shall (at its sole cost and expense): (i) defend and/or settle on behalf of Customer (including Customer's officers, directors, employees, representatives and agents); and (ii) indemnify Customer for, any third party claims brought 6 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 against Customer based upon a claim that Customer's use of the Products in accordance with this Agreement infringes or misappropriates such third party's intellectual property rights in a jurisdiction which is signatory to the Berne Convention. (ii) By Customer. Customer shall (at its sole cost and expense): (i) defend and/or settle on behalf of Tenable (including Tenable's officers, directors, employees, representatives and agents) and (ii) indemnify Tenable for, any third party claims brought against Tenable arising out of or relating to Customer's use of the Products to perform Scans on third party Scan Targets, except to the extent that any such claim or action is caused by a failure of the Products to materially comply with the Documentation. (b) In Case of Infringement. If Customer's use of the Products is, or in Tenable's opinion is likely to be, the subject of an infringement claim, Tenable may, in its sole discretion and expense: (i) modify or replace the infringing Products as necessary to avoid infringement, provided that the replacement Products are substantially similar in functionality; (ii) procure the right for Customer to continue using the infringing Products; or (iii) terminate this Agreement and, upon Customer's return or certified destruction of the infringing Product, provide Customer a pro-rata refund calculated as follows: (x) for infringing Products licensed on a subscription basis, the refund shall consist of any prepaid but unused fees for the remainder of the applicable License Term; or (y) for infringing Software licensed on a perpetual basis or infringing Hardware, the refund shall consist of a straight line depreciation of the license fee based on a three (3) year useful life as well as any prepaid but unused fees for separately charged Support Services. This Section 9 sets forth Tenable's sole and exclusive liability and Customer's sole and exclusive remedy with respect to any claim of intellectual property infringement. (c) Exclusions. Tenable shall have no liability with respect to a third party intellectual property infringement claim arising out of: (i) modifications of the Product made by Customer or a party under its control to conform with Customer's specifications; (ii) modifications of the Product made by anyone other than Tenable or a Tenable authorized third party; (iii) Customer's use of the Product in combination with other products or services not provided by Tenable; (iv) Customer's failure to use any updated versions of the Product made available by Tenable; or (v) Customer's use of the Product in a manner not permitted by this Agreement or otherwise not in accordance with the Documentation. (d) Requirements. The indemnitor shall only be responsible for the indemnification obligations set forth in this Section 9 if the indemnitee: (i) provides the indemnitor prompt written notice of such action or claim; (ii) gives the indemnitor the right to control and direct the investigation, defense, and/or settlement of such action or claim; (iii) reasonably cooperates with the indemnitor in the defense of such a claim (at the indemnitor's expense); and (iv) is not in breach of this Agreement. Nothing herein shall prevent the indemnitee from engaging in defense of any such claim with its own legal representation, provided that this does not materially prejudice the indemnitor's defense. The indemnitor may not settle any claim on behalf of the indemnitee without obtaining the indemnitee's prior written consent; provided, however, the indemnitor shall not be required to obtain consent to

settle a claim which settlement consists solely of: (x) discontinued use of infringing Products and/or (y) the payment of money for which the indemnitor has a duty to indemnify.

10. Legal Compliance. (a) Generally. The Products are intended solely for lawful purposes and use. Both Parties, and their agents and Affiliates, agree to perform their respective obligations in an ethical manner that complies with all applicable national, federal, state and local laws, statutes, ordinances, regulations and codes ("Applicable Laws") including, without limitation, the Computer Fraud and Abuse Act (CFAA), 18 USC Sec. 1030, the U.S. Foreign Corrupt Practices Act of 1977, as amended, and the UK Bribery Act of 2010. If Customer violates this Section 10, Tenable may terminate this Agreement immediately. (b) Trade Controls. Applicable Laws include U.S. export laws (including the International Traffic in Arms Regulation (ITAR), 22 CFR 120-130, and the Export Administration Regulation (EAR), 15 CFR Parts 730 et seq.) and the anti-boycott rules implemented by the Departments of Commerce and Treasury. Information regarding export classifications of Tenable's Products may be found on its website (www.tenable.com/export-controls or a successor location). Customer agrees that it will be the exporter of record any time it causes the Products to be accessed outside the United States or by a national of any country other than the United States. The Parties further agree to comply with trade and economic sanctions, rules, and regulations of the United States, European Union, EU member states, United Kingdom and other applicable government authorities and shall not engage in prohibited trade to persons or entities who are the subject of an active sanction, embargo, or executive order. Customer hereby acknowledges and confirms that Customer (including Customer's officers, directors, employees, representatives and agents): (i) is not included on, owned or controlled by an individual or entity included on, or acting on behalf of an individual or entity included on any of the restricted party lists maintained by the U.S. Government (e.g., Specially Designated Nationals List, Foreign Sanctions Evader List, Sectoral Sanctions Identification List, Denied Persons List, Unverified List, Entity List or List of Statutorily Debarred Parties) (collectively, "Restricted Parties"); (ii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use by or for Restricted Parties; (iii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use in, by or for countries or territories subject to U.S. economic sanctions (e.g., Crimea, Cuba, Iran, North Korea, or Syria); or (iv) will not use or sell the Products…

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Hayes e-Government Resources

Solution Name: Critical Start - Cyber Operations Risk and Response 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.

Critical Start's Cyber Operations Risk and Response Platform (CORR) is Critical Start's proprietary SOAR platform used to deliver Managed Detection and Response (MDR) services. CORR leverages bi-directional API integrations to collect security alerts from clients' EDR, XDR and SIEM platforms. CORR resolves 99.9% of false positive alerts through a zero trust model that allows our RSOC to eliminate alert fatigue, resolve false positives at scale, and provide targeted intelligence to alerts. The CORR platform and services allow organizations to offload initial triage of security alerts as well as enable the Critical Start team to provide real-time Repsonse functions including host isolation, AV Scan, file blocks and more, directly from the CORR portal. Critical Start's zero trust model ensures that ALL alerts are actioned and provides clients with a more complete view of their security posture while ensuring security teams are not overwhelmed by alert volume or overlooking security incidents being masked by numerous false positives.

The Critical Start platform supports EDR tools to include Microsoft Defender for Endpoint, Sentinel One, CrowdStrike and Palo Alto Cortex as well as XDR functionality from Microsoft Defender XDR and Palo Alto. SIEM integrations supported include Microsoft Sentinel, Splunk Cloud, Sumo Logic and Devo, if deployed. Critical Start also offers its own logging platform, Managed XDR for organzations which do not have or want their own SIEM.

Ongoing services included with the platform include:

- Correlation and analysis of Security Alerts from the supported technologies

- Leverging the Trusted Behvior Registry, Critical Start automatically resolves known-good activity, vastly reducing false positives.

- Investigation of alerts by the Critical Start Security Operations Center on a 24x7x365 basis

- Alert enrichment providing additional context on IP addresses, file hashes and domain names

- Threat Navigator, a platform capability that maps threat detection to the MITRE ATT&CK framework

- Highly customizable Response actions, based on the integrated technologies, to provide accelerated containment and mitigation of threats, when identified

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.

Critical Start offers a Managed XDR solution as an optional component of our Managed Detection and Response (MDR) capabilities. The Managed XDR platform allows clients to collect logs from numerous IT security platforms including firwalls, IDS/IPS, cloud services, etc. Critical Start's Threat Engineering team applies any available out-of-the-box threat detections as well as developing additional correlations to alert on any identified indicators of compromise.

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.

Critical Start implements a well-defined workflow for incident handling, including alerting, investigation, and response. The workflow begins with the analysis of every event generated by the client's security tools using the Trusted Behavior Registry (TBR). Any event determined through previous investigation to be a false positive is auto-resolved by TBR. All other events, either unknown or malicious, are escalated to the Critical Start SOC for human analysis.

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.

Critical Start works be integrating with customer security tools. We receive alerts from your tools and build detections into your security tech stack that look at all possible suspicious behaviors. These are noisy and prone to generating false positives, but allow us to see activity ignored by other SOCs. We eliminate the traditional problem of alert fatigue through our Trusted Behavior Registry (TBR) which automatically resolves false positives and allow us to identify anomalous behavior.

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.

Yes, Critical Start empowers users to create personalized dashboards and reports. There are five types of dashboards available: Situational Awareness, Recent Activity, Your Team Performance, Critical Start Service Efficiency, and a Custom Dashboard. The Custom Dashboard displays a wide variety of metrics so users can choose those most important to them. Additionally, specific time values can be set for the view to walk through analysis of trends over time.

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.

Critical Start's RSOC will respond and triage all incidents discovered during the investigation. Response activities include but are not limited to: isolating an infected host, stopping a malicious process, and running virus scans. After the attack is contained or eliminated, alerts are escalated to the client for notification. Escalations include a full breakdown of actions taken by the RSOC and any next actions. Clients can contact the RSOC at any time.

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.

CORR does not currently support direct ingestion of Threat Intel feeds, however, Critical Start has fully capable Cyberthreat Research Unit and Security Engineering teams to research new and emerging threats and vulnerabilities, then build new detections from these findings.

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.

Critical Start's Cyber Threat Intelligence (CTI) team subscribes to both paid and open-source threat intelligence feeds to collect and curate threat data. The specific commercial feeds are not currently public information. The CTI team researches and reports on new threats and suspicious TTPs requiring Critical Start and customer action. They feed this data to the Threat Detection Engineering team to develop new detections.

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.

Critical Start's Service Level Agreements (SLAs) include a 60-minute Time to Detect (TTD) and 60-minute Median Time to Resolution (MTTR), which includes TTD within it. There is also a 10-minute Critical Alert Notification SLA.

Platform and Mobile application availability is at 99.9%.

If these SLAs are not met, service credits are provided as per the terms in our Service Agreement.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Hayes e-Government Resources

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.

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Hayes e-Government Resources

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.

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 efficiency.

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 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 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 enhancing decision-making.

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 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 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.

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

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L7 – Service Category 7: Security Operations Platform

Respondent Name: Hayes e-Government Resources

Solution Name: Tenable - One

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.

Tenable One serves as a robust Security Operations Platform (SOP) designed to unify diverse security tools & technologies into a single, cohesive platform, delivering extensive visibility into an organization's IT environment. Built with a focus on integration & comprehensive security insights, Tenable One enables security teams to detect, investigate, & respond to threats providing a holistic view of security incidents through intelligent data correlation across the entire attack surface.

Tenable One integrates seamlessly with a range of security tools, SIEM, asset discovery, & threat intelligence platforms. This integration creates a single, centralized platform where all relevant data is aggregated, allowing security teams to view the organization's entire threat l&scape within one interface. This unified view eliminates the need for manual data collection & minimizes the risk of overlooking critical security information.

Leveraging Tenable's Threat Intelligence, Tenable One continuously monitors for potential threats. By correlating vulnerability & asset data, Tenable One identifies risks based on asset criticality & exposure, enabling security teams to prioritize threats effectively. This monitoring capabilities facilitates faster threat detection & provides comprehensive investigative insights, empowering security teams to address incidents proactively.

Tenable One enhances incident response by providing contextual information about threats, asset details, & vulnerability prioritization, which enables teams to focus on the most critical incidents first. By automating workflows, alerting mechanisms, & reporting, Tenable One reduces the mean time to detect (MTTD) & mean time to respond (MTTR) to incidents. This streamlined response helps security teams maintain an agile, informed approach to threat management.

With Tenable One, security teams gain access to detailed analytics & reporting capabilities, which include dashboards that provide insight into risk trends & threat patterns. These analytics support data driven decision making & enable a more strategic approach to security. Tenable One's visualization tools empower stakeholders to underst& the overall security posture, fostering better collaboration & prioritization across teams.

Tenable One is designed to support organizations of varying sizes & can scale to meet the needs of exp&ing infrastructures. This scalability ensures that the platform continues to provide comprehensive visibility & effective threat management as the organization grows, without compromising on performance or data integrity.

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.

Tenable One enhances the State's log correlation by integrating with SIEM tools like Splunk & QRadar, adding contextual risk data to support threat detection. It aggregates vulnerability information & applies risk prioritization, allowing security teams to focus on high-impact threats. Tenable One's threat intelligence & anomaly detection aid in identifying indicators of compromise, complementing the SIEM's capabilities to detect patterns, providing a unified view.

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.

Although Tenable One does not natively provide this, we do integrate with Security Orchestration, Automation, & Response (SOAR) platforms to automate incident response tasks like blocking IPs, isolating devices, & generating alerts. This integration enables security teams to streamline workflows & respond swiftly to threats. ￼

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.

The Attack Path Analysis feature identifies & evaluates potential pathways through which vulnerabilities might be exploited. Tenable provides both a CVSS & Vulnerability Priority Rating (VPR) scoring for each vulnerability that is discovered, using a risk based approach to help customer prioritize which vulnerabilities present the greatest risk, based on the probability that they will be leveraged in an in an actual attack in the near future & potential loss impact.

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.

Tenable uses dashboards, which are made from widgets of data, to provide views & display information that is easy to read, consume, & understand. Dashboards are interactive, graphical interfaces that often provide at-a-glance views of key performance indicators. Dashboards can be shared with other users & exported to PDF & other formats on an ad-hoc or scheduled basis as required. In addition, scheduled exports can then be emailed to configured

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.

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 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.

Tenable ingests data from various threat intelligence feeds to predict what is most likely to be exploited and have the greatest impact in the next 28 days and assigns multiple risk ranking scores. An automated process analyses all the raw data on each vulnerability–including its age, availability of exploits & exploit kits, presence in ExploitDB & Metasploit, & whether it's being actively discussed on the dark web, in forums &/or on social media, etc.

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.

Tenable One's capabilities for providing comprehensive threat context, identifying potential attack vectors, & conducting exploit pathway & blast-radius assessments make it a powerful tool for proactive threat management. By leveraging advanced features such as Attack Path Analysis, MITRE ATT&CK framework integration, & enriched asset metadata, Tenable One ensures that organizations can effectively manage & mitigate security 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.

SLA: Uptime Guarantee:

Service Level Agreement for Hosted Services This Service Level Agreement ("SLA") between Tenable ("Tenable") and Customer is subject to the applicable license or subscription agreement between Tenable and Customer under which the Customer licenses the Hosted Services, or if the parties have not executed such separate agreement, the Tenable Master Agreement located at http://static.tenable.com/prod_docs/tenable_slas.html (the "Agreement"). All defined terms used in this SLA and not defined herein shall have the meaning assigned to them in the Agreement. Tenable shall provide the Hosted Services and Software in connection with the Agreement. This SLA governs Tenable's performance and delivery of the Hosted Services to Customer.

1. Definitions.

"Potential Uptime" means the amount of time in a given month. "Production Uptime" represents the amount of time in a given month that Customer has the ability to log in or access the Hosted Services user interface (or authenticate to APIs) and perform associated Scanning related activity. Potential Uptime is measured by Tenable in a given month by the following calculation: Production Uptime = (Potential Uptime – Hosted Services Interruption Time) / (Potential Uptime – Exclusions) "Hosted Services Interruption Time" is the period of time for which the Hosted Services (or any material portion thereof) are unavailable due to issues caused by or attributable to Tenable or its agents. Hosted Services Interruption Time does not include Regular Maintenance or Scheduled Maintenance. "Regular Maintenance" is the period of time under which the Hosted Services may be unavailable for recurring maintenance work. Tenable attempts to schedule this time when usage of the Hosted Services is light across Tenable's customer base and therefore, Tenable shall use commercially reasonable efforts to only conduct Regular Maintenance daily between the hours of 7AM and 9AM (ET) and non-business days. Regular Maintenance is required in order to update Tenable's plug-in databases as well as to maintain system health requirements. Tenable shall use commercially reasonable efforts to minimize any Regular Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Regular Maintenance. "Scheduled Maintenance" is the period of time under which the Hosted Services may be unavailable for non-recurring maintenance. Scheduled Maintenance is required in order to provide updates to the Hosted Services as well as to maintain system health requirements. Tenable shall provide Customer at least twelve (12) hours advance notice prior to Scheduled Maintenance; provided, however, Tenable shall endeavor to provide at least twenty-four (24) hours advanced notice for Scheduled Maintenance. Notice for Scheduled Maintenance will be provided at the following URL or successor location: status.tenable.com. Tenable shall use commercially reasonable efforts to minimize any Scheduled Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Scheduled Maintenance. "Emergency Maintenance" describes maintenance for certain emergency situations, where

advance notice may be not be feasible, possible or practical. Tenable shall use commercially reasonable efforts to minimize any Emergency Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Periods of Emergency Maintenance shall be included in Hosted Services Interruption Time. Tenable Confidential and Proprietary SLA v.3

2. Service Levels Commitment. Tenable commits to provide a 99.95% Production Uptime with respect to the Hosted Services during each calendar month of the subscription term.

3. Service Level Credits. If Tenable fails to perform the Hosted Services in accordance with the Service Level Commitment, then Customer may request a Service Level Credit in accordance with this SLA. Service Level Credits shall be Customer's sole and exclusive remedy for unavailability or performance degradation of the specific Hosted Services.

4. Weighting Factor. The "Weighting Factor" for calculation of the Service Level Credit is set forth below and correlates to the relative unavailability of the Hosted Service in a given month.

Production Uptime between 99.95% and 100% = 0 Production Uptime between 95.00% and 99.94% = .1 Production Uptime between 90.00% and 94.99% = .15 Production Uptime below 90% = .2

5. Calculation of Service Level Credits. The following equation shall be used to calculate any Service Level Credits: Service Level Credit (in $) = Weighting Factor multiplied by the monthly fee for applicable Hosted Service.

Example: Production Uptime in a given month is 95%. The monthly fee for the Hosted Service is $100 (Annual fee for the Hosted Services is $1,200). Service Level Credit (in $) = (0.1) x $100 = $10.

If Customer has paid in advance for one or more years of the Hosted Services, monthly fees will be calculated on a pro rata basis.

6. Exclusions. "Exclusions" shall mean any time for which the Hosted Services are unavailable to do any of the following: (i) Customer's breach of, or failure to perform any obligations under, this SLA or the Agreement; (ii) issues relating to Customer's environment, internal networks, computer systems, firewalls or Customer's inability to connect to the internet; (iii) Force Majeure Events; or (iv) issues arising from failures, acts or omissions Tenable's upstream service providers (i.e. AWS).

7. Requests. In order to receive a Service Level Credit, Customer must request such by emailing Tenable at credits@tenable.com, within 10 days of the end of the applicable month. If Customer is past due or in default with respect to any payment or any material contractual obligations to Tenable, Customer is not eligible for any Service Level Credit. Service Level Credits are non-refundable and may only be applied to future upgrades or renewals of the specific Tenable Hosted Services affected.

8. Changes. This Service Level Commitment may be amended by Tenable in its reasonable discretion but only after providing thirty (30) days' advance notice. Tenable may provide such notice either as a note on the screen presented upon logging in to the Hosted Services, by posting updated terms on Tenable's website, or by email to the email addressed registered with Customer's account. This SLA was updated on October, 2023 (ver 3).

Master Agreement, accepted via a click-thru acknowledgement at time of installation:

Due to the document exceeding the allotted character limit, the full documentation can be located at https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf . We have included what we can below.

TENABLE MASTER AGREEMENT This Master Agreement (this “Agreement”) is made by and between Tenable (as defined below) and the customer licensing Products and/or receiving services (“Customer”) with an effective date as of the date Customer clicks to accept this Agreement (the “Effective Date”). Hereinafter, each of Tenable and Customer may be referred to collectively as the “Parties” or individually as a “Party”.

1. Definitions. (a) “Affiliate” means any entity that controls, is controlled by, or is under common control with a Party. “Control” shall mean: (1) ownership (either directly or indirectly) of greater than fifty percent (50%) of the voting equity or other controlling equity of another entity; or (2) power of one entity to direct the management or policies of another entity, by contract or otherwise. (b) “Documentation” means the then-current official user manuals and/or documentation for the Products available at docs.tenable.com (or a successor location). (c) “Hosted Services” are a type of service offered through Tenable’s cloud-based software as a service (SaaS) platform and include Scans and access to and use of the hosted environment (the “Hosted Environment”). (d) “Product(s)” means any of the products that Tenable offers, including Software, Hosted Services, Hardware (if any), Support Services and Professional Services. (e) “Professional Services” means services purchased, including consulting services which are relevant to the implementation and configurations of Tenable Products as well as on-site or virtual training courses. Generally, Professional Services are defined either in a separate SOW or a Services Brief. Professional Services do not include the Hosted Services or Support Services. (f) “Scan(s)” are a function performed by the Software and/or the Hosted Services on Scan Targets, which are conducted in order to provide data to Customer regarding its network security. “PCI Scans” are a specific type of Scan designed to assess compliance with the Payment Card Industry Data Security Standard. “Scan Data” is the resulting information created by the Scan. “Scan Target(s)” are the targets or subjects of a Scan. (g) “Services Brief” means the document which outlines Tenable’s basic, pre-packaged installation or training Professional Services offered under a Tenable SKU and which do not require a separate SOW. Current versions of Services Briefs may be found at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). For the avoidance of doubt, Customer may purchase commercial off the shelf SKU-based Professional Services without executing a separate Statement of Work. A “SOW” or “Statement of Work” shall further describe Professional Services, the terms of which may be customized and which shall require execution by the Customer. (h) “Software” means each software product made available by Tenable under this Agreement for download. Software includes patches, updates, improvements, additions, enhancements and other modifications or revised versions of the same that may be provided to Customer by Tenable from time to time. (i) “Technical Data” means data Customer uploads or runs through or on the Products, or is otherwise generated thereby, including information regarding licensing metrics and product behavioral data. (j) “Tenable” means: (i) Tenable, Inc., if Customer is a commercial entity or individual located in North or South America (Tenable, Inc. is a Delaware corporation having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); (ii) Tenable 2 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 Public Sector LLC, if Customer is an agency or instrumentality of the United States Government, a commercial entity operating predominantly as a federal systems integrator

for eventual sale or resale or for the benefit of the United States Government, or an agency or instrumentality of a State or local government within the United States (Tenable Public Sector LLC is a Delaware limited liability company having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); or (iii) Tenable Network Security Ireland Limited, if Customer is located outside of North or South America (Tenable Network Security Ireland Limited is a private limited company having offices at 81b Campshires, Sir John Rogerson's Quay, Dublin 2, Ireland).

2. Orders and Transactions. (a) Reseller Transactions. If Customer purchases Tenable Products through an authorized Tenable reseller (a "Reseller"), all terms related to pricing, billing, invoicing and payment ("Payment Terms") set forth in this Agreement (if any) shall not apply. For the avoidance of doubt, all such Payment Terms shall be as agreed to between Customer and Reseller. To place an order, Customer shall provide the Reseller with a purchase order (or other similar document acceptable to Reseller) in response to a valid quote from such Reseller. Following Reseller's receipt of such purchase order, Tenable shall issue a sales order confirmation or other similar order acceptance document (the "Ordering Document"). No order shall be deemed accepted by Tenable until Tenable issues the Ordering Document. The Ordering Document shall set forth all Products (and corresponding licensing metrics) purchased by Customer. (b) Direct Transactions. If the Parties have agreed to transact directly, the following Payment Terms shall apply. Customer agrees to pay all amounts due as specified in a Tenable invoice. Fees for Hosted Services are charged for access to the Host Environment (as defined herein), not actual usage. Payment is due within thirty (30) days from the date of Tenable's invoice to Customer. Customer will pay directly or reimburse Tenable for any taxes (including, sales or excise taxes, value added taxes, gross receipt taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, imposed on or arising out of this Agreement. Notwithstanding the foregoing, Tenable will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. Customer agrees to pay Tenable without deducting any present or future taxes, withholdings or other charges except those deductions it is legally required to make. If Customer is legally required to make any deductions or withholding, Customer agrees to provide evidence of such withholding upon request. If a certificate of exemption or similar document or proceeding is necessary in order to exempt any transaction from a tax, Customer shall provide such certificate or document to Tenable. (c) Delivery and Installation. Delivery of Tenable Products ("Delivery") shall be deemed to occur on the date of availability for electronic download or electronic access. Tenable has no duty to provide installation services for Tenable Products unless installation services are purchased separately.

3. Term and Termination. (a) Agreement Term. This Agreement shall commence upon the Effective Date and continue until terminated in accordance with the terms set forth herein. (b) License Term and Renewals. The "License Term" is the term of the license or subscription for Products as set forth in the Ordering Document. If this Agreement has been signed by both Parties, then unless otherwise agreed to in writing, any License Term, including renewals, shall be governed by the terms set forth herein. If this Agreement has been accepted via shrinkwrap or click through, upon any renewal of the License Term, the terms then available at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location) will govern such renewal. Customer agrees that use of the Products at the time of such renewal will be deemed full and adequate acceptance of the updated terms. (c) Termination for Cause. Either Party may terminate this Agreement for cause if the other Party materially breaches this Agreement provided that such breaching Party has received written notice of such breach and failed to cure such breach within thirty (30) days. If this Agreement is terminated for cause by either Party, Customer

shall remove all copies of the Products from any Customer systems and cease to use any Software or Hosted Services purchased hereunder. Further, Customer shall certify to Tenable that it has returned or destroyed all copies of the Software. If this Agreement is terminated for cause by Tenable, Customer shall remain responsible for any outstanding payment obligations throughout the rest of the License Term. (d) Termination for Convenience. Customer may terminate this Agreement for any lawful reason upon ninety (90) days' prior written notice to Tenable. If Customer terminates for convenience, Customer shall not receive a refund and shall remain obligated to pay for Products for which it has previously entered into a transaction as well as any additional payment obligations agreed upon prior to the termination date.

4. Products. (a) Product-Specific Terms. Pursuant to this Agreement, Customer may receive the right to use various Products as further described in the attached schedules (each, a "Schedule"). Terms related to Customer's use of Software are described in Schedule A 3 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 (Software). Terms related to Customer's use of Hosted Services are described in Schedule B (Hosted Services). Terms related to the provision of Professional Services are described in Schedule C (Professional Services). For each Product, Customer will have the right to use the corresponding Documentation. (b) Licensing Model. Product licenses shall be in accordance with the terms of the applicable licensing model as set forth in the Documentation and/or the Ordering Document, which may include limitations on Scan Targets, compute, storage, resource utilization, License Term, the number of users, seats, licenses and/or types of modules licensed. Product licenses shall commence upon Delivery and shall be either perpetual or subscription in nature. Tenable shall use commercially reasonable efforts to meter resource utilization and assess likeness or uniqueness of Scan Targets within each Product/module licensed. If Customer exceeds the license restrictions, Customer must purchase an upgraded license to allow for all actual or additional usage, and Tenable or its Reseller may promptly invoice Customer for any such overages at a price not to exceed Tenable's then-current rates. Discrepancies in Scan Target or utilization count is the sole responsibility of the Customer to resolve. (c) Restrictions on Use. Customer shall not directly or indirectly: (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive, obtain or modify the source code of the Products; (ii) reproduce, modify, translate or create derivative works of all or any part of the Products; (iii) remove, alter or obscure any proprietary notice, labels, or marks on the Products; (iv) without Tenable's prior written consent, use the Products in a service bureau, application service provider or similar capacity; (v) without signing Tenable's Managed Security Services Provider Addendum, use the Products to provide any managed service to a third party; (vi) use the Products in order to create competitive analysis or a competitive product or service; (vii) copy any ideas, features, functions or graphics in the Product; or (viii) without Tenable's prior written consent, interfere with or disrupt performance of Hosted Services (e.g., perform penetration testing on Tenable systems). Customer may only use the Products to manage or gather information from Scan Targets owned or hosted by Customer or its Affiliates, or third parties for which Customer has received express authorization to Scan. (d) Intellectual Property in Products. This Agreement does not transfer to Customer any title to or any ownership right or interest in the Products. Any rights in the Products not expressly granted in this Agreement are reserved by Tenable. If Customer provides Tenable with any comments, suggestions, or other feedback regarding the Product, Customer hereby assigns to Tenable all right, title and interest in and to such feedback. For clarity, such feedback shall not contain Customer Confidential Information and shall not reference or identify Customer or its users. (e) Customer Requirements. In order to use the Products, Customer must meet or exceed the specifications found in the

Documentation. (f) Product Features. Customer agrees that purchase of any Product is not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Tenable regarding future functionality or features. Tenable reserves the right to withdraw features from future versions of the Products provided that: (i) the core functionality of the affected Product remains the same; or (ii) Customer is offered access to a product or service providing materially similar functionality as the functionality removed from the affected Product. The preceding remedies under this Section 4(f) are the sole remedies available if Tenable withdraws features from the Products. (g) Rights Granted to Tenable. Provided that Tenable shall not publicly disclose any Customer Confidential Information, Tenable may: (i) use Technical Data for reasonable business purposes, including Support Services, license validation, research and development, feature creation, and Product testing; (ii) include aggregated and anonymized Technical Data in public materials; and (iii) retain Technical Data which is anonymized after the termination of this Agreement. (h) Hardware. Any Hardware purchased under this Agreement (if any) will be subject to the terms and conditions of Schedule D located at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). (i) Temporary Limitation. If Tenable reasonably believes: (i) Customer's use of the Products places an unreasonable or disproportionate burden on the Products; (ii) Customer's use of the Products poses a risk or threat to the Products (including any systems supporting the Products), Tenable, or a third party; or (iii) Customer's usage exceeds the limitations of the license, then Tenable may temporarily limit Customer's access to or use of the Products or any specific feature therein. Tenable may also suspend or limit access to the Products if Customer fails to make any payments related to this Agreement. Tenable will, to the extent practical under the circumstances, use commercially reasonable efforts to provide Customer with prior written notice of any such limitation (email or in product messaging shall be sufficient). When commercially reasonable, Tenable shall promptly restore access once the Customer has remediated the issue. For the avoidance of doubt, Customer is responsible for all normal fees during any period for which usage or access is limited pursuant to this section. (j) Additional Details on Use Restrictions for Tenable Security Network Ireland Limited. The following shall only apply for transactions with Tenable Security Network Ireland Limited. Notwithstanding anything in Section 4(c), decompiling the Product is 4 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 permitted to the extent the laws of Customer's jurisdiction give Customer the right to do so to obtain information necessary to render the Products interoperable with other software; provided, however, that Customer must first request such information from Tenable and Tenable may, in its discretion, either provide such information to Customer or impose reasonable conditions, including a reasonable fee, on such use of the Products to ensure that its proprietary rights in the Product are protected.

5. Support. (a) Support Services. Tenable shall provide Customer with support services (the "Support Services") in accordance with Tenable's then-current Technical Support Plans (available at http://static.tenable.com/prod_docs/tenable_slas.html or a successor location) and consistent with Tenable's End of Life and End of Sale definitions contained therein. The Support Services include bug fixes, updates (including new vulnerability plug-ins), or enhancements that Tenable makes generally available to users of the Products. The Support Services also include the provision of new minor (Example: 1.1.x to 1.2.x, etc.) and major version releases of the Products (Example: 1.x to 2.x, etc.). (b) Support Fees. Standard Support Services for Products licensed for a finite License Term will be provided at no additional charge beyond the license fee for the duration of the License Term. Support Services for Products licensed on a perpetual basis must

be purchased separately in advance. In all cases, premium support may be purchased at an additional charge. If during the course of a perpetual license Customer terminates or fails to renew the Support Services, Customer may, at any time during the term of this Agreement, request that Tenable reinstate the Support Services provided that Customer pays for the lapsed Support Services in an amount equal to the total fees Customer would have paid for the Support Services between the time Customer's Support Services lapsed and the then-current date.

6. Confidentiality. (a) Definition. "Confidential Information" means information learned or disclosed by a Party under this Agreement that should reasonably be assumed to be confidential or proprietary, including the Products and the terms of this Agreement. Confidential Information will remain the property of the disclosing Party, and the receiving Party will not be deemed by virtue of this Agreement or any access to the Confidential Information to have acquired any right, title or interest in or to the Confidential Information. (b) Obligations. Each Party agrees to only use the Confidential Information in connection with this Agreement or a purchase hereunder. The receiving Party agrees to hold the disclosing Party's Confidential Information confidential using at least the same level of protection against unauthorized disclosure or use as the receiving Party normally uses to protect its own information of a similar character, but in no event less than a reasonable degree of care. Each Party may share Confidential Information with its Affiliates or authorized contractors in the performance of its duties under this Agreement; provided, however, that each Party shall be responsible to ensure that such Affiliate or authorized contractors are bound by obligations of confidentiality at least as stringent as those set forth in this Agreement. (c) Exclusions. Confidential Information shall not include information that: (i) is already known to the receiving Party free of any confidentiality obligation; (ii) is or becomes publicly known through no wrongful act of the receiving Party; (iii) is rightfully received by the receiving Party from a third party without any restriction or confidentiality; or (iv) is independently developed by the receiving Party without reference to the Confidential Information. Confidential Information does not include Scan Data that has been aggregated or anonymized so that it is not attributable to the disclosing Party. If Customer requests or performs scans on third party Scan Targets, and such third party inquires with Tenable about the scan, Tenable shall inform Customer and allow Customer to resolve any disputes with the third party. If Customer fails to contact the third party, Customer agrees that Tenable may provide Customer's business contact information to the owner of the Scan Targets as well as to relevant authorities, and such disclosure shall not be considered a breach of confidentiality. (d) Sensitive Information. The Parties agree that Customer's disclosure of sensitive, personal information (e.g., social security numbers, national identity card numbers, personal credit card information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and health care data) ("Sensitive Information") is not required for Tenable to perform its duties under this Agreement or sell any Products hereunder. If Customer inadvertently or unintentionally discloses any Sensitive Information to Tenable, Customer shall identify to Tenable that it has disclosed Sensitive Information and Tenable shall promptly return and/or destroy such Sensitive Information. (e) Legal Disclosures; Remedies. The receiving Party may disclose Confidential Information if required to do so by law provided the receiving Party shall promptly notify the disclosing Party so that the disclosing Party may seek any appropriate protective order and/or take any other action to prevent or limit such disclosure. If required hereunder, the receiving Party shall furnish only that portion of the Confidential Information disclosure of which is legally required. The receiving Party acknowledges and agrees that the breach of any term, covenant or provision of this Agreement may cause irreparable harm to the disclosing Party and, accordingly, upon the threatened or

actual breach by the receiving Party of any term, covenant or provision of this Agreement, the disclosing Party shall 5 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 be entitled to seek injunctive relief, together with any other remedy available at law or in equity. The receiving Party will notify the disclosing Party promptly of any unauthorized use or disclosure of the disclosing Party's Confidential Information.

7. Representations and Warranties; Disclaimer. (a) Warranty of Authority. The Parties hereby represent and warrant that they have the full power and authority to enter into this Agreement. (b) Products. Product warranties and associated warranty periods are set forth in the relevant Schedules. (c) Antivirus Warranty. Tenable represents it has taken commercially reasonable efforts to ensure that the Products, at the time of Delivery, are free from any known and undisclosed virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that would erase data or programming or otherwise cause the Products to become inoperable or incapable of being used in the manner for which it was designed or in accordance with the Documentation. (d) Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT AND TO THE GREATEST EXTENT PERMITTED BY LAW, TENABLE OFFERS ITS PRODUCTS "AS-IS" AND MAKES NO OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF TITLE, NON INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SECURITY, INTEGRATION, PERFORMANCE AND ACCURACY, AND ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. THE WARRANTIES SET FORTH IN THIS AGREEMENT ARE MADE TO CUSTOMER FOR CUSTOMER'S BENEFIT ONLY. CUSTOMER'S USE OF THE PRODUCTS IS AT CUSTOMER'S OWN RISK. CUSTOMER UNDERSTANDS THAT ASSESSING NETWORK SECURITY IS A COMPLEX PROCEDURE, AND TENABLE DOES NOT GUARANTEE THAT THE RESULTS OF THE PRODUCTS WILL BE ERROR-FREE OR PROVIDE A COMPLETE AND ACCURATE PICTURE OF CUSTOMER'S SECURITY FLAWS, AND CUSTOMER AGREES NOT TO RELY SOLELY ON SUCH PRODUCTS IN DEVELOPING ITS SECURITY STRATEGY. CUSTOMER ACKNOWLEDGES THAT THE PRODUCTS MAY RESULT IN LOSS OF SERVICE OR HAVE OTHER IMPACTS TO NETWORKS, ASSETS OR COMPUTERS (INCLUDING MODIFICATION OF SCAN TARGETS), AND CUSTOMER IS SOLELY RESPONSIBLE FOR ANY DAMAGES RELATING TO SUCH LOSS OR IMPACT.

8. Limitation of Liability. (a) Direct Damages. The cumulative liability of one Party to the other for all claims arising from or relating to the Products or this Agreement (including without limitation, any cause of action sounding in contract, tort or strict liability) shall be limited to proven direct damages in an amount not to exceed, in the aggregate, the fees paid by Customer for the Products over the twelve (12) months immediately prior to the event giving rise to the claim. (b) Indirect Damages. Neither Party shall be liable to the other for any indirect, incidental, special, punitive, consequential or exemplary damages regardless of the nature of the claim. This prohibition on indirect damages shall include, but not be limited to, claims based on lost profits, cost of delay, any failure of Delivery, business interruption, cost of lost or damaged data, or liabilities to any third parties even if such Party is advised of the possibility thereof. (c) Carve Outs. The liability caps set forth in Sections 8(a) and 8(b) shall not apply to damages resulting from: (i) personal injury or death; (ii) fraud or willful misconduct; (iii) indemnification obligations set forth in Section 9 (Indemnification); or (iv) Customer's breach of Section 4(c) (Restrictions on Use). (d) Limitations; Time Period. Each of the limitations set forth in this Section 8 shall be enforced to the

fullest extent of the law. Any laws preventing such limitations shall only apply to the extent required by law and the remaining unaffected terms shall apply in full. Unless expressly prohibited by law, each Party shall have a period of no greater than twelve (12) months from the date the cause of action accrues to bring a claim against the other Party for such cause of action.

9. Indemnification. (a) Indemnification Obligations. (i) By Tenable. Tenable shall (at its sole cost and expense): (i) defend and/or settle on behalf of Customer (including Customer's officers, directors, employees, representatives and agents); and (ii) indemnify Customer for, any third party claims brought 6 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 against Customer based upon a claim that Customer's use of the Products in accordance with this Agreement infringes or misappropriates such third party's intellectual property rights in a jurisdiction which is signatory to the Berne Convention. (ii) By Customer. Customer shall (at its sole cost and expense): (i) defend and/or settle on behalf of Tenable (including Tenable's officers, directors, employees, representatives and agents) and (ii) indemnify Tenable for, any third party claims brought against Tenable arising out of or relating to Customer's use of the Products to perform Scans on third party Scan Targets, except to the extent that any such claim or action is caused by a failure of the Products to materially comply with the Documentation. (b) In Case of Infringement. If Customer's use of the Products is, or in Tenable's opinion is likely to be, the subject of an infringement claim, Tenable may, in its sole discretion and expense: (i) modify or replace the infringing Products as necessary to avoid infringement, provided that the replacement Products are substantially similar in functionality; (ii) procure the right for Customer to continue using the infringing Products; or (iii) terminate this Agreement and, upon Customer's return or certified destruction of the infringing Product, provide Customer a pro-rata refund calculated as follows: (x) for infringing Products licensed on a subscription basis, the refund shall consist of any prepaid but unused fees for the remainder of the applicable License Term; or (y) for infringing Software licensed on a perpetual basis or infringing Hardware, the refund shall consist of a straight line depreciation of the license fee based on a three (3) year useful life as well as any prepaid but unused fees for separately charged Support Services. This Section 9 sets forth Tenable's sole and exclusive liability and Customer's sole and exclusive remedy with respect to any claim of intellectual property infringement. (c) Exclusions. Tenable shall have no liability with respect to a third party intellectual property infringement claim arising out of: (i) modifications of the Product made by Customer or a party under its control to conform with Customer's specifications; (ii) modifications of the Product made by anyone other than Tenable or a Tenable authorized third party; (iii) Customer's use of the Product in combination with other products or services not provided by Tenable; (iv) Customer's failure to use any updated versions of the Product made available by Tenable; or (v) Customer's use of the Product in a manner not permitted by this Agreement or otherwise not in accordance with the Documentation. (d) Requirements. The indemnitor shall only be responsible for the indemnification obligations set forth in this Section 9 if the indemnitee: (i) provides the indemnitor prompt written notice of such action or claim; (ii) gives the indemnitor the right to control and direct the investigation, defense, and/or settlement of such action or claim; (iii) reasonably cooperates with the indemnitor in the defense of such a claim (at the indemnitor's expense); and (iv) is not in breach of this Agreement. Nothing herein shall prevent the indemnitee from engaging in defense of any such claim with its own legal representation, provided that this does not materially prejudice the indemnitor's defense. The indemnitor may not settle any claim on behalf of the indemnitee without obtaining the indemnitee's prior written consent; provided, however, the indemnitor shall not be required to obtain consent to

settle a claim which settlement consists solely of: (x) discontinued use of infringing Products and/or (y) the payment of money for which the indemnitor has a duty to indemnify.

10. Legal Compliance. (a) Generally. The Products are intended solely for lawful purposes and use. Both Parties, and their agents and Affiliates, agree to perform their respective obligations in an ethical manner that complies with all applicable national, federal, state and local laws, statutes, ordinances, regulations and codes (“Applicable Laws”) including, without limitation, the Computer Fraud and Abuse Act (CFAA), 18 USC Sec. 1030, the U.S. Foreign Corrupt Practices Act of 1977, as amended, and the UK Bribery Act of 2010. If Customer violates this Section 10, Tenable may terminate this Agreement immediately. (b) Trade Controls. Applicable Laws include U.S. export laws (including the International Traffic in Arms Regulation (ITAR), 22 CFR 120-130, and the Export Administration Regulation (EAR), 15 CFR Parts 730 et seq.) and the anti-boycott rules implemented by the Departments of Commerce and Treasury. Information regarding export classifications of Tenable’s Products may be found on its website (www.tenable.com/export-controls or a successor location). Customer agrees that it will be the exporter of record any time it causes the Products to be accessed outside the United States or by a national of any country other than the United States. The Parties further agree to comply with trade and economic sanctions, rules, and regulations of the United States, European Union, EU member states, United Kingdom and other applicable government authorities and shall not engage in prohibited trade to persons or entities who are the subject of an active sanction, embargo, or executive order. Customer hereby acknowledges and confirms that Customer (including Customer’s officers, directors, employees, representatives and agents): (i) is not included on, owned or controlled by an individual or entity included on, or acting on behalf of an individual or entity included on any of the restricted party lists maintained by the U.S. Government (e.g., Specially Designated Nationals List, Foreign Sanctions Evader List, Sectoral Sanctions Identification List, Denied Persons List, Unverified List, Entity List or List of Statutorily Debarred Parties) (collectively, “Restricted Parties”); (ii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use by or for Restricted Parties; (iii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use in, by or for countries or territories subject to U.S. economic sanctions (e.g., Crimea, Cuba, Iran, North Korea, or Syria); or (iv) will not use or sell the Products…

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L8 – Service Category 8: Identity and Access Management (IAM)

Respondent Name: Hayes e-Government Resources

Solution Name: CyberArk - Identity

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.

CyberArk Identity Lifecycle Management automates and streamlines the entire lifecycle of user identities, from onboarding to de-provisioning, ensuring secure and efficient access control.

Lifecycle Management

1. **Onboarding**:

- **Automated Provisioning**: New users are automatically provisioned with the necessary access rights based on their roles and attributes. Integration with HR systems like Workday or BambooHR ensures that user data is up-to-date and accurate.

- **Self-Service Portals**: Users can request access to applications through self-service portals, reducing the burden on IT helpdesks

2. **Access Management**:

- **Role-Based Access Control (RBAC)**: Access rights are assigned based on user roles, ensuring that users have the appropriate permissions for their job functions. This simplifies management and enhances security by limiting access to only what is necessary.

- **Attribute-Based Access Control (ABAC)**: Access decisions are made based on user attributes (e.g., department, location), allowing for more granular and dynamic access control.

3. **Ongoing Management**:

- **Dynamic Provisioning**: As users change roles or departments, their access rights are automatically updated to reflect their new responsibilities.

- **Approval Workflows**: Automated workflows ensure that access requests are reviewed and approved by the appropriate personnel, maintaining compliance and security.

4. **De-Provisioning**:

- **Automated Deactivation**: When users leave the organization, their access rights are automatically revoked, reducing the risk of unauthorized access.

- **Audit and Reporting**: Comprehensive reporting tools track access activity and help ensure compliance with security policies.

Enforcing Access Control

- **RBAC**: Simplifies access management by grouping users into roles with predefined permissions. This approach is efficient for managing large numbers of users with similar access needs.

- **ABAC**: Provides a more flexible and context-aware access control mechanism by evaluating user attributes and environmental conditions. This allows for dynamic and fine-grained access decisions.

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.

CyberArk Identity seamlessly integrates with both on-premise and cloud applications, providing a unified platform for secure access. It reduces password fatigue by enabling single sign-on (SSO) and passwordless authentication, allowing users to log in once and access multiple applications without repeatedly entering credentials. This ensures a smooth and efficient login experience.

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.

CyberArk Identity's MFA solution supports various authentication methods, including TOTP, SMS, and biometrics. Users can authenticate via one-time passcodes from mobile apps, SMS confirmation codes, and biometric methods like fingerprint or facial recognition. This flexibility ensures robust security and user convenience.

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.

CyberArk Identity uses Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to provide fine-grained access permissions. RBAC assigns permissions based on user roles, while ABAC uses attributes like location, department, or security clearance to dynamically grant access. This combination ensures precise control over who can access what resources, enhancing security and compliance.

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.

CyberArk Identity enables cross-domain authentication by acting as an Identity Provider (IdP) using standard protocols like SAML, OAuth, and OpenID Connect. It verifies user identities and issues tokens or assertions that applications can trust, facilitating secure single sign-on (SSO) and access management across different domains.

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.

CyberArk Identity integrates with CyberArk PAM and EPM to control and monitor admin accounts by providing single sign-on (SSO) and multi-factor authentication (MFA) for secure access. It ensures that privileged access is limited and audited through detailed session monitoring, automated workflows, and compliance reporting.

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.

CyberArk Identity and Workforce Password Management (WPM) allow users to manage their passwords, request access to systems, and track access requests. Users can reset passwords, request system access, and monitor request status through an approval workflow. Approvers can grant or deny access, ensuring secure and efficient access management.

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.

CyberArk Identity integrates with CyberArk Workforce Password Management (WPM) and Endpoint Privilege Manager (EPM) to enhance security. WPM manages and monitors credentials, detecting anomalies and compromised credentials. EPM enforces least privilege, blocks suspicious activities, and contains threats at the endpoint. Together, they provide real-time detection and response to identity threats.

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.

CyberArk Identity SaaS uptime SLA is 99.99%

CyberArk Service Availability Service Level Agreement

This Service Availability Service Level Agreement ("SLA") is incorporated into and subject to the CyberArk SaaS Terms of Service (the "SaaS Terms"). Unless otherwise provided herein, all capitalized terms will have the meaning specified in the SaaS Terms. CyberArk reserves the right to change the terms of this SLA from time to time.

Availability Commitment. CyberArk shall use commercially reasonable efforts to make the SaaS Product (excluding any locally installed agents or connectors) (the "Service") available at an Uptime Percentage as set forth in Annex 1 (the "Availability Commitment"). As used herein, "Uptime Percentage" means the total number of minutes in a calendar month minus the number of minutes of Unavailability (excluding Unavailability associated with any SLA Exclusion) incurred in a calendar month, divided by the total number of minutes in a calendar month. "Unavailable" and "Unavailability" are defined per SaaS Product, as set forth in Annex 1. The Availability Commitment of each Service is measured independently.

Service Credits. In the event CyberArk does not meet the Availability Commitment, Customer shall be eligible to receive a credit ("Service Credit"). Service Credits are calculated as a percentage of the pro-rated monthly subscription fee paid to CyberArk for the affected SaaS Product for the Subscription Term in which the Unavailability occurred, and based on the actual Uptime Percentage, as detailed in Annex 1. The receipt of a Service Credit is CyberArk's sole liability and Customer's exclusive remedy for CyberArk's failure to meet the Availability Commitment.

Credit Request. In order to receive a Service Credit, Customer must submit a request that reasonably details the claimed Unavailability, by opening a ticket in CyberArk Customer Portal, within fourteen (14) days following the end of the calendar month in which the Unavailability occurred. CyberArk shall review the request, and if it confirms, acting reasonably and in good faith, that the actual Uptime Percentage of the Service referenced in the request did not meet the Availability Commitment, CyberArk will provide Customer with a Service Credit, applicable against future fees payable by Customer. In the event that Customer does not renew its then-current Subscription Term of the applicable SaaS Product and has no outstanding payments due to CyberArk, then Customer shall be entitled to receive a refund of the Service Credit. A Service Credit may not be transferred to other CyberArk customers.

SLA Exclusions. The Availability Commitment does not apply to any Unavailability arising from (i) factors outside of CyberArk's reasonable control, including but not limited to, any force majeure event, Internet access, electrical disruptions; (ii) Customer's network, on-premise environment and related components (including, access to Customer's hosted encryption keys, operating systems, software and platforms); (iii) any equipment, software or other technology other than those within CyberArk's direct and sole control; (iv) connectivity issues due to any firewall, censorship infrastructure, internet monitoring tool, or internet filter utilized, operated or otherwise deployed by the Customer or any third party, including but not limited to, any government agency, regulatory body or statutory body; (v) necessary risk mitigation actions undertaken in response to external threats (such as DDOS attack attempts); (vi) use of the SaaS Product in violation of the SaaS Terms or Documentation; (vii) CyberArk's suspension and/or termination of Customer's right to use the SaaS Product in accordance with the SaaS Terms; or (viii) any Service Maintenance (collectively, "SLA Exclusions"). As used herein, "Service Maintenance" means

(i) routine weekly maintenance performed by CyberArk on Sundays during 3:30am-6:00am Eastern Time (EST or EDT, as appropriate) and for any Customer whose tenant is hosted on a data center located in the Asia-Pacific & Japan region, also from Sunday 10:00pm to Monday 12:30am SGT; (ii) other system upgrades and enhancements performed if announced in product, on the SaaS Product's status page, the Service customer portal or via email, at least two days in advance; or (iii) emergency maintenance outside of the routine or pre-scheduled maintenance window that is reasonably required to apply patches or fixes, or to undertake other urgent maintenance activities. CyberArk will make reasonable efforts to limit the Service Maintenance window to the minimum possible to avoid disruption to the Service.

Annex 1

Uptime Percentage per SaaS Product

SaaS Product - Uptime Percentage

All SaaS Products available as of the date hereof, except as specifically mentioned in this table- 99.9%

Privilege Cloud - 99.95%

Remote Access - 99.95%

Dynamic Privilege Access - 99.95%

Endpoint Privilege Manager - 99.95%

Cloud Entitlements Manager - 99.95%

Secure Cloud Access - 99.95%

Identity - 99.99%

.

SAAS SUBSCRIPTION AND SERVICES AGREEMENT

Due to the document exceeding the allotted character limits, the full documentation can be located at "SaaS-and-Services-Agmt--CYBR-Global--20240517". We have included what we can below.

This SAAS SUBSCRIPTION AND SERVICES AGREEMENT ("Agreement") is made as of the later signing date below (“Effective Date”) by and between CyberArk and ____________ incorporated and registered in __________ and having a place of business at _____________ ("Customer"), each a “Party” and both the “Parties.” Capitalized terms used herein are defined in the “Definitions and Interpretation” section of this Agreement.

Background: Customer wishes to purchase certain SaaS Products and Professional Services as stated in the applicable Order or SOW entered into by the Parties pursuant to the terms of this Agreement. In consideration of their mutual promises and other good and valuable consideration, the Parties agree as follows:

1. Access and Use

1.1. Access and Use. CyberArk grants Customer, during the Subscription Term, a non-exclusive, non-transferable right to access and use (and permit Authorized Users of Customer and its Affiliates to access and use) the SaaS Products and applicable Documentation solely for Customer’s and its Affiliates’ internal business purposes in accordance with the Documentation and in the quantity specified in the applicable Order. Such license grant is subject to payment of all applicable fees set forth in the Order or payment in accordance with an Indirect Order through a Channel Partner (as appropriate) and the terms and conditions of this Agreement. CyberArk may update or upgrade the SaaS Products from time-to-time.

1.2. Access and Use Restrictions. Customer shall not (directly or indirectly): (a) copy or reproduce the SaaS Products or the Documentation except as permitted under this Agreement; (b) exceed the subscribed quantities, Authorized users or other entitlement measures of the SaaS Products as set forth in the applicable Order; (c) remove or destroy any copyright, trademark or other proprietary marking or legends placed on or contained in the SaaS Products, Documentation or CyberArk Intellectual Property; (d) assign, sell, sublicense, distribute or otherwise transfer or make available the rights granted to Customer under this Agreement to any third party except as expressly set forth herein; (e) modify, reverse engineer or disassemble the SaaS Products; (f) except to the limited extent applicable laws specifically prohibit such restriction, decompile, attempt to derive the source code or underlying ideas or algorithms of any part of the SaaS Products, attempt to recreate the SaaS Products or use the SaaS Products for any competitive or benchmark purposes; (g) create, translate or otherwise prepare derivative works based upon the SaaS Products, Documentation or CyberArk Intellectual Property; (h) interfere with or disrupt the integrity or performance of the SaaS Products; (i) attempt to gain unauthorized access to the SaaS Products or its related systems or networks, or perform unauthorized penetrating testing on the SaaS Products; (j) use the SaaS Products in a manner that infringes on the Intellectual Property rights, publicity rights, or privacy rights of any third party, or to store or transfer defamatory, trade libelous or otherwise unlawful data; or (k) except as otherwise agreed by the Parties in the applicable BAA, store in or process with the SaaS Products any personal health data, credit card data, personal financial data or other such sensitive regulated data not required by the Documentation, or any Customer Data that is subject to the International Traffic in Arms Regulations maintained by the United States Department of State. Fees for the SaaS Products are based on use of the SaaS Products in a manner consistent with the

Documentation. If Customer uses, or is reasonably suspected of using, the SaaS Products in violation of the Documentation or exceeding the licensed quantities or other entitlement measures as set forth in an applicable Order, Customer shall cooperate with CyberArk to resolve any non-compliance, which may include payment for any such overages at then-current applicable rates.

1.3. Login Access to the SaaS Products. Customer is solely responsible for ensuring: (i) that only appropriate Authorized Users have access to the SaaS Products; (ii) that such Authorized Users have been trained in proper use of the SaaS Products; and (iii) proper usage of passwords, tokens and access procedures with respect to logging into the SaaS Products. CyberArk may refuse registration of or suspend Customer's or a specific user's access and use of the SaaS Products if CyberArk knows or reasonably suspects that Customer's access or use is malicious or otherwise harmful to the Customer itself, the SaaS Products or CyberArk's other customers. CyberArk will provide notice prior to such suspension if permitted by applicable law and unless CyberArk reasonably believes that providing such notice poses a risk to the security of the SaaS Products. CyberArk will promptly reinstate Customer's access and use once the issue has been resolved.

1.4. Professional Services License. Subject to full and final payment for Professional Services (either directly or in accordance with section 2.3 “Indirect Orders”) and the terms of this Agreement, CyberArk grants Customer a non-exclusive, non-transferable, non-assignable license to use (and to permit its Authorized Users to use) solely for Customer's and its Affiliates' internal use any Intellectual Property provided by CyberArk to Customer as a result of, or otherwise incorporated into, the Professional Services (excluding the SaaS Products).

1.5. Third Party Materials. The SaaS Products include Third-Party Materials, use of which is subject to their respective OSS Licenses as indicated in the Documentation. CyberArk warrants that the inclusion of such Third-Party Materials in the SaaS Products will not prevent Customer from exercising the license rights provided to Customer herein in respect of the SaaS Products or limit Customer's ability to use the SaaS Products in accordance with the Documentation. Nothing herein shall derogate from mandatory rights Customer may have under any OSS Licenses, if any. Customer may obtain a copy of the source code for certain Third-Party Materials by following the instructions set forth in the Documentation.

1.6. Support. As part of its provision of the SaaS Products, CyberArk shall make available technical support to Customer in accordance with the Support Services terms applicable to the SaaS Products. Upon notification from CyberArk, Customer shall promptly; update any Agents on Customer systems that interact with the SaaS Products; and/or as applicable, ensure that all Authorized Users download and install all available updates for locally installed components without undue delay. Customer acknowledges and agrees that its failure to timely install such updates may result in disruptions to or failures of the SaaS Products, security risks or suspension of Customer's access to the SaaS Products, without any liability on the part of CyberArk to Customer.

1.7. SaaS Product Usage Analytics. CyberArk and its Affiliates shall be permitted to collect and use Usage Analytics for its reasonable business purposes and for Customer's benefit (including research and development, statistical analyses, monitoring and management of CyberArk's products). Other than for the purpose of providing the SaaS Products to Customer, in the event CyberArk discloses Usage Analytics or any part thereof to third parties (either during the Subscription Term or thereafter) such data shall be deidentified so that it will not identify Customer or its Authorized Users. The foregoing shall not limit in any way CyberArk's confidentiality obligations pursuant to section 4 below.

2. Payment and Taxes

2.1. Payment Terms. Without prejudice to Customer's rights set out elsewhere in this Agreement, all SaaS Products fees are non-refundable and payable in advance. CyberArk may invoice: (a) for purchases of SaaS Products, upon delivery; and (b) for Professional Services (if applicable), according to the nature of the Professional Services: (i) upon CyberArk's receipt of the applicable Order for the Professional Services; (ii) monthly as rendered; or (iii) as otherwise set forth in the applicable Order or SOW. Where:

(A) Customer is paying CyberArk directly, Customer shall pay all invoices within thirty (30) days of date of invoice, without any deduction or set-off (except for any amount disputed promptly and in writing by Customer in good faith), and payment will be sent to the address specified by CyberArk. Any amounts arising in relation to this Agreement not paid when due will be subject to a late charge of one and one-half percent (1 ½ %) per month on the unpaid balance or the maximum rate allowed by law, whichever is less; or

(B) Customer places an Indirect Order, CyberArk grants the rights described in this Agreement in consideration for and subject to: (a) Customer's agreement to comply with the pricing and payment terms of the Indirect Order, to be separately agreed between Customer and the applicable Channel Partner; and (b) Customer's agreement to comply with its obligations set forth in this Agreement (including the restrictions on use of the SaaS Products).

Notwithstanding the foregoing, the final sales price or rate shall be freely and independently determined between the applicable Channel Partner and Customer. For the avoidance of doubt, in the case of such an Indirect Order, any indication in this Agreement of an agreement between Customer and CyberArk for the price payable by Customer for such Indirect Order shall be null and void and not form a binding part of this Agreement and the provisions of this Agreement related to payment terms, pricing and/or order procedures shall not apply.

2.2. Taxes. The fees and charges covered by this Agreement are exclusive of any Indirect Taxes imposed or levied, currently or in the future based on applicable legislation, on the SaaS

Products and Professional Services. Unless otherwise agreed between the Parties, Customer will be liable for compliance with reporting and payment of such Indirect Taxes in its tax jurisdiction. CyberArk shall include the Indirect Taxes on its invoice to Customer and remit such Indirect Taxes collected to the relevant authority if required by applicable law. For the avoidance of doubt, CyberArk will be responsible for direct taxes imposed on CyberArk's net income or gross receipts in its tax jurisdiction. Notwithstanding the forgoing, all payments made under this Agreement shall be in cleared funds, without any deduction or set-off, and free and clear of and without deduction from any Indirect Taxes or other withholdings of any nature.

3. Rights in Intellectual Property

3.1. Intellectual Property. Except for the rights granted in this Agreement, all rights, title, and interest in and to the SaaS Products, Documentation, and CyberArk Intellectual Property are hereby reserved by CyberArk, its Affiliates or licensors. Except as provided for herein, all rights, title, and interest in and to Customer Intellectual Property are hereby reserved by Customer, its Affiliates or licensors. Nothing in this Agreement shall transfer ownership of any Intellectual Property rights from one Party to the other. Customer shall not prohibit or enjoin CyberArk at any time from utilizing any skills or knowledge of a general nature acquired during the course of providing Professional Services, including using information publicly known or made available or that could reasonably be acquired in similar work performed for another customer of CyberArk.

3.2. Customer Data. Customer owns all right, title and interest in all Customer Data. Nothing in this Agreement shall be construed to grant CyberArk any rights in Customer Data beyond those expressly provided herein. Customer grants CyberArk and its Affiliates the limited, non-exclusive, worldwide license to view and use the Customer Data for the purpose of providing and improving the SaaS Products.

3.3. Suggestions. To the extent that Customer provides CyberArk with Suggestions, such Suggestions shall be free from any confidentiality restrictions that might otherwise be imposed upon CyberArk pursuant to this Agreement, and may be implemented by CyberArk in its sole discretion. Customer acknowledges that any CyberArk products or materials incorporating any such Suggestions shall be the sole and exclusive property of CyberArk.

3.4. AI Features. Certain features within the SaaS products use algorithmic analysis, artificial intelligence and/or machine learning technologies ("AI Features"). Use of the AI Features is subject to the Documentation and CyberArk's Responsible AI Policy found at https://www.cyberark.com/trust/responsible-ai/. Information regarding opting-out of AI Features is located in the Documentation.

4. Confidentiality

4.1. Confidential Information. The Parties acknowledge that each may disclose certain valuable confidential and proprietary information to the other Party. The receiving Party may only use the disclosing Party's Confidential Information to fulfil the purposes of this Agreement and in accordance with the terms of this Agreement. The receiving Party will protect the disclosing Party's Confidential Information by using at least the same degree of care as the receiving Party uses to protect its own Confidential Information of a like nature (but no less than a reasonable degree of care) to prevent the unauthorized use, dissemination, disclosure or publication of such Confidential Information. Notwithstanding the foregoing, the receiving Party may disclose Confidential Information to its (and its Affiliates) employees, advisors, consultants and agents on a need-to-know basis and provided that such party is bound by obligations of confidentiality substantially similar to those contained herein. This section 4 supersedes any and all prior or contemporaneous understandings and agreements, whether written or oral, between the Parties with respect to Confidential Information and is a complete and exclusive statement thereof. Additionally, the obligations set forth in section 5.4 and not this section 4 herein apply to Customer Data.

4.2. Exceptions. Information will not be deemed Confidential Information if it: (i) is known to the receiving Party prior to receipt from the disclosing Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (ii) becomes known (independently of disclosure by the disclosing Party) to the receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the disclosing Party; (iii) becomes publicly known or otherwise ceases to be secret or confidential, except through a breach of this Agreement by the receiving Party; or (iv) is independently developed by the receiving Party without use of or reliance upon the disclosing Party's Confidential Information and the receiving Party can provide evidence to that effect. The receiving Party may disclose Confidential Information pursuant to the requirements of a court, governmental agency or by operation of law but shall (to the extent permissible by law) limit such disclosure to only the information requested and give the disclosing Party prior written notice sufficient to permit the disclosing Party to contest such disclosure.

4.3. Advertising and Publicity. Neither Party shall make or permit to be made any public announcement concerning the existence, subject matter or terms of this Agreement or the relationship between the Parties without the prior written consent of the other Party except as expressly permitted in this section. Customer grants CyberArk and its Affiliates during the term of the Agreement the right to use Customer's trade names, logos, and symbols ("Customer Marks") in its public promotional materials and communications for the sole purpose of identifying Customer as a CyberArk customer. CyberArk shall not modify the Customer Marks, or display the Customer Marks any larger or more prominent on its promotional materials than the names, logos, or symbols of other CyberArk customers. The foregoing promotional materials and communications may be created, displayed, and reproduced without Customer's review, provided that they are in compliance with this section and any Customer Marks usage guidelines provided by Customer to CyberArk in writing.

5. Security and Processing of Personal Data

5.1. Customer Data Content. As between CyberArk and Customer, Customer is solely responsible for: (i) the content, quality and accuracy of Customer Data as made available by Customer and by Authorized Users; (ii) providing notice to Authorized Users with regards to how Customer Data will be collected and used for the purpose of the SaaS Products; (iii) ensuring Customer has a valid legal basis for processing Customer Data and for sharing Customer Data with CyberArk (to the extent applicable); and (iv) ensuring that the Customer Data as made available by Customer complies with applicable laws and regulations including (where applicable) Applicable Data Protection Laws.

5.2. Data Protection Laws. The Parties shall comply with their respective obligations under the Applicable Data Protection Laws. In particular, if Customer is established in the European Economic Area ("EEA"), in Switzerland, in the United Kingdom ("UK") or in California, or will, in connection with the SaaS Products, provide CyberArk with personal data relating to an individual located within the EEA, Switzerland the UK or California, the Parties shall comply with the Data Processing Addendum found at https://www.cyberark.com/CyberArk-Data-Processing-Addendum.pdf ("DPA") which in such case is hereby incorporated into this Agreement.

5.3. HIPAA (Health Insurance Portability and Accountability Act). To the extent that (a) Customer is established in the United States; and (b) is a "covered entity" or a "business associate" and includes "Protected Health Information" (as these terms are defined in the Business Associate Agreement ("BAA")) in Customer Data, the Parties shall comply with the BAA found at https://www.cyberark.com/lgl/CyberArk-BAA.pdf. In such case, the terms of the BAA are hereby incorporated into this Agreement by reference.

5.4. Security of Customer Data. CyberArk shall: (i) ensure that is has in place appropriate administrative, physical and technical measures designed to protect the security and confidentiality of Customer Data against any accidental or illicit destruction, alteration or unauthorized access or disclosure to third parties; and (ii) access and use the Customer Data solely to perform its obligations in accordance with the terms of this Agreement, and as otherwise expressly permitted in this Agreement. CyberArk shall not materially diminish its security controls with respect to Customer Data during a particular SaaS Products term. The obligations set forth in this Section 5.4 are in addition to any confidentiality, privacy, security or other requirements contained in the BAA or DPA, as applicable.

5.5. Bring Your Own Key. If Customer chooses to enable the "Bring Your Own Key" functionality for data encryption made available by CyberArk for certain SaaS Products ("BYOK"), Customer acknowledges that (i) Customer shall bear sole responsibility for the hosting, use, protection, rotation and management of such encryption key and any loss, damage, unavailability or non-performance resulting therefrom; (ii) Customer shall provide CyberArk with access to the encryption key at all times in order to encrypt Customer Data and proper performance of the SaaS Products; and (iii) CyberArk has no control over the encryption key and specifically is unable to de-encrypt, restore, recover or otherwise retrieve Customer Data in the event the encryption key is lost, damaged or otherwise not made available to CyberArk. If BYOK functionality is enabled by Customer, CyberArk disclaims any and all responsibility and liability for unavailability or non-performance of the SaaS Products caused by loss, damage or any unavailability of the encryption key.

6. Warranties

6.1. Limited SaaS Products Warranty. During the applicable Subscription Term, CyberArk warrants that: (a) the SaaS Products will perform in substantial conformity with the Documentation, and (b) CyberArk will use industry standard measures designed to detect viruses, worms, Trojan horses or other unintended malicious or destructive code in the SaaS Products. The foregoing warranties are void if the failure of the SaaS Products has resulted from negligence, error, or misuse of the SaaS Products (including use not in accordance with the Documentation) by Customer, the Authorized User or by anyone other than CyberArk. Customer shall be required to report any breach of warranty to CyberArk within a period of thirty (30) days of the date on which the incident giving rise to the claim occurred. CyberArk's sole and exclusive liability, and Customer's sole and exclusive remedy, for breach of these warranties will be for CyberArk, at its expense, to use reasonable commercial efforts to correct such nonconformity within thirty (30) days of the date that notice of the breach was provided; and, if CyberArk fails to correct the breach within such cure period, Customer may terminate the affected Order and, in such event, CyberArk shall provide Customer with a pro-rata refund of any unused pre-paid fees paid for the period following termination as calculated on a monthly basis for the affected SaaS Products. Without derogating from CyberArk's obligations under this Agreement, Customer warrants that it shall take and maintain appropriate steps within its control to protect the confidentiality, integrity, and security of its Confidential Information and Customer Data, including: (i) operating the SaaS Products in accordance with the Documentation and applicable law and; and (ii) dedicating reasonably adequate personnel and resources to implement and maintain the security controls set forth in the Documentation. Customer will be responsible for the acts and omissions of its Authorized Users.

6.2. Professional Services Warranty. CyberArk warrants that: (a) it is competent and possesses the necessary expertise and financial resources to perform the Professional Services; (b) the Professional Services will be performed in a professional and workmanlike manner, consistent with reasonably applicable industry standards; and (c) all personnel performing Professional Services shall have suitable training, education, experience, know-how and skill to perform the relevant Professional Services in a competent manner. Customer shall notify CyberArk in writing of any claims under the foregoing Professional Services warranties within five (5) business days following CyberArk's performance of the defective Professional Services.

6.3. Compliance with Law. Each Party shall comply with all applicable, laws and regulations in connection with the performance of its obligations and the exercise of its rights under this Agreement.

6.4. Disclaimer. Any and all warranties, expressed, incorporated or implied are limited to the extent and period mentioned in this Agreement. To the maximum extent allowed by applicable law, CyberArk disclaims (and disclaims on behalf of its licensors and/or contributors to any Third-Party Materials) all other warranties, conditions and other terms, whether express or implied or incorporated into this Agreement by statute, common law or otherwise, including the implied conditions and warranties of merchantability and fitness for a particular purpose. CyberArk will have no responsibility or liability for delays, failures or losses (i) attributable or related in any way to the use or implementation of third-party hardware, software or services not provided by CyberArk; or (ii) use of the SaaS Products not in accordance with the Documentation.

7. Indemnification

7.1. Infringement Indemnity. CyberArk shall defend and indemnify Customer and/or its Affiliates and their officers, directors and employees against all third-party claims, suits and proceedings and all directly related losses, liabilities, damages, costs and expenses (including reasonable attorneys' fees) resulting from the violation, misappropriation, or infringement of such third party's patent, copyright, trademark or trade secret caused by Customer's use of the SaaS Products in accordance with this Agreement and the Documentation.

7.2. Customer Data and Use Indemnity. Customer shall defend and indemnify CyberArk and/or its Affiliates and their officers, directors and employees against any third-party claims, suits and proceedings (including those brought by a government entity), and all directly related losses, liabilities, damages, costs and expenses (including reasonable attorneys' fees), resulting from: (i) an alleged infringement or violation by the Customer Data of such third-party's patent, copyright, trademark, trade secret; or (ii) CyberArk's use of the Customer Data violating applicable law, provided that such use is in accordance with the terms of this Agreement and (where applicable) with the terms of the DPA and/ or the BAA.

7.3. Process. Each Party's defense and indemnification obligations herein will become effective upon, and are subject to: (a) the indemnified Party's prompt notification to the indemnifying Party of any claims in writing; and (b) the indemnified Party providing the indemnifying Party with full and complete control, authority and information for the defense of the claim, provided that the indemnifying Party will have no authority to enter into any settlement or admission of the indemnified Party's wrongdoing on behalf of the indemnified Party without the indemnified Party's prior written consent (not to be unreasonably withheld). At the indemnifying Party's request, the indemnified Party shall reasonably cooperate with the indemnifying Party in defending or settling any claim.

7.4. Exclusions. The above CyberArk obligations to defend and indemnify will not apply in the event that a claim arises from or relates to: (a) use of the SaaS Products not in accordance with the Documentation and this Agreement; (b) use of the SaaS Products in violation of applicable laws; (c) any modification, alteration or conversion of the SaaS Products not created or approved in writing by CyberArk; (d) any combination of the SaaS Products with any computer, hardware, software, data or service not provided by CyberArk; (e) CyberArk's compliance with specifications, requirements or requests of Customer; or (f) Customer's gross negligence or willful misconduct.

7.5. Remedies. If a SaaS Product becomes, or CyberArk reasonably determines that a SaaS Product is likely to become, subject to a claim of infringement for which CyberArk must indemnify Customer as described above, CyberArk may at its option and expense: (a) procure for Customer the right to continue to access and use that SaaS Product; (b) replace or modify that SaaS Product so that it becomes non-infringing without causing a material adverse effect on the functionality provided by that SaaS Product; or (c) if neither of the foregoing options are available in a timely manner on commercially reasonable terms, terminate the affected Order and provide Customer with a pro-rata refund of any unused pre-paid fees paid for the period following termination as calculated on a monthly basis for that SaaS Product. This section titled "Indemnification" states the sole liability of CyberArk and the exclusive remedy of Customer with respect to any indemnification claims arising out of or related to this Agreement.

8. Limitation of Liability

8.1. Maximum Liability. Except for liability caused by CyberArk's intellectual property infringement indemnification obligations in section 7.1, Customer's data infringement indemnity in section 7.2, or Customer's payment obligations herein, in no event will either Party's maximum aggregate liability arising out of or related to this Agreement, regardless of the cause of action and whether in contract, tort (including negligence), warranty, indemnity or any other legal theory, exceed the total amount paid or payable to CyberArk under this Agreement during the twelve (12) month period preceding the date of initial claim.

8.2. No Consequential Damages. Neither Party will have any liability to the other Party for any loss of profits or revenues, loss of goodwill, or for any indirect, special, incidental, consequential or punitive damages arising out of, or in connection with this Agreement, however caused, whether in contract, tort (including negligence), warranty, indemnity or any other legal theory, and whether or not the Party has been advised of the possibility of such damages.

8.3. Construction. This Agreement is not intended to and will not be construed as excluding or limiting any liability which cannot be limited or excluded by applicable law, including liability for: (a) death or bodily injury caused by a Party's negligence; or (b) gross negligence, willful misconduct, or fraud.

9. Restricted Rights and Export Control

9.1. Export Control. The exportation of the SaaS Products and Documentation, and all related technology and information thereof are subject to U.S. laws and regulations pertaining to export controls and trade and economic sanctions, including the U.S. Export Administration Act, Export Administration Regulations, the Export Control Reform Act, and the Office of Foreign Assets Control's sanctions programs, the laws of the State of Israel, and the laws of any country or organization of nations within whose jurisdiction Customer (or its Authorized Users who may use or otherwise receive the SaaS Products as expressly authorized by this Agreement) operates or does business, as amended, and the rules and regulations promulgated from time to time thereunder. Specifically, Customer hereby undertakes not to export, re-export, access or grant access to the SaaS Products and all related technology, information, materials and any upgrades thereto to: (a) any Prohibited Persons; (b) any country to which such export, re-export or access from is restricted or prohibited per the foregoing applicable laws; or (c) otherwise in violation of any applicable export or import restrictions, laws or regulations. Customer also certifies that it is not a Prohibited Person nor owned, controlled by, or acting on behalf of a Prohibited Person.

9.2. Commercial Computer Software and FedRAMP Products. If Customer is an agency or contractor of the United States Government, Customer acknowledges and agrees that: (i) the SaaS Products (including any software forming a part thereof) were developed entirely at private expense; (ii) the SaaS Products (including any software forming a part thereof) in all respects constitute proprietary data belonging solely to CyberArk; (iii) the SaaS Products (including any software forming a part thereof) are not in the public domain; and (iv) the software forming a part of the SaaS Products is “Commercial Computer Software” as defined in sub-paragraph (a)(1) of DFARS section 252.227-7014 or FAR Part 12.212. Customer shall provide no rights in the Software (including any software forming a part thereof) to any U.S. Government agency or any other party except as expressly provided in this Agreement. If Customer places an Order for SaaS Products which are designated as “FedRAMP Authorized,” the CyberArk Rider to SaaS Terms of Service for FedRAMP Products found at https://www.cyberark.com/contract-terms/ is incorporated herein and will apply to CyberArk’s provision of such SaaS Products.

10. Professional Services. If Customer purchases Professional Services, this section titled “Professional Services” will apply. In the event of a conflict between any provisions of the Agreement and a SOW, the provisions of the SOW will govern with respect to the specific Professional Services described therein.

10.1. Performance; Personnel. CyberArk will perform the Professional Services on a time and materials and non-exclusive basis, or as otherwise detailed in the relevant Order or SOW, and as more particularly detailed in the relevant SOW. Customer will provide reasonable support, services, material, facilities and other items…

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L10 – Service Category 10: Secure Access Service Edge (SASE)

Respondent Name: Hayes e-Government Resources

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.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L10 – Service Category 10: Secure Access Service Edge (SASE)

Respondent Name: Hayes e-Government Resources

Solution Name: Zscaler - Zero Trust Exchange

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.

Zscaler's architecture acts as an exchange/switchboard to connect any user, branch office, device, and workload using business policies over any network to any application..

As the only fully integrated SSE platform, Zscaler's SASE leverages the Zero Trust Exchange, a cloud-native architecture that unifies security functions to provide seamless connectivity for remote users, branch offices, and cloud applications across the State's digital environment.

The SASE solution includes a full suite of security services: SWG, CASB with integrated DLP, ZTNA, FWaaS, IPS, Browser Isolation, Sandbox, SSL inspection, Advanced Threat Protection, Bandwidth Control, URL Filtering, and flexible policy management. Together, these components provide comprehensive threat protection, visibility, and policy enforcement, securing the State's data and resources.

Zscaler's platform fully integrates the aforementioned, creating a single proxy for efficient, low-latency processing across data flows. The integrated DLP engine delivers consistent data protection, enabling Florida to enforce data security policies effectively in a scalable, cloud-native environment tailored to specific subscription levels.

Zscaler's SASE operates entirely in the cloud, removing the need for traditional hardware. This architecture simplifies deployment, scales automatically, and reduces latency to enhance the experience for all State users. Our SASE solution integrates with 3rd party SD-WAN or Zscaler Secure SD-WAN to route traffic dynamically across public and private links based on real-time network conditions. This ensures high performance for critical applications, while simplifying network management by selecting optimal paths automatically.

The SWG inspects internet-bound traffic in real-time, blocking malicious sites, phishing, and other threats, allowing secure web access for users without physical security appliances. The CASB provides visibility and control over cloud applications, allowing Florida to enforce security policies on popular SaaS platforms. This includes integrated DLP and activity monitoring, protecting sensitive data even in external cloud environments.

ZTNA enforces the Zero Trust model, requiring users and devices to authenticate for each session. By segmenting access based on identity and role, ZTNA enables granular control over app access, aligning with Florida's goal to reduce risk exposure. FWaaS offers centralized, cloud-based firewall protection against internal and external threats. Unlike traditional firewalls, FWaaS is optimized for encrypted traffic and scales to handle high volumes, enabling efficient threat detection while meeting Florida's security protocols.

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.

Zscaler integrates SD-WAN with policy-based routing to optimize network paths based on real-time conditions and application needs. It enables dynamic path selection across public and private links, ensuring top performance for critical applications. Context-aware routing policies manage latency, bandwidth, and security, providing high-quality connectivity for users across cloud applications and remote sites. Centralized, cloud-based policies streamline SD-WAN operations.

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.

ZPA is a secure SaaS solution that enforces least-privilege access by connecting users only to authorized applications based on identity and context, such as user role, device health, and location. By avoiding network-based trust, ZPA secures access to on-premise or cloud applications without exposing the network. Unlike VPNs, ZPA eliminates direct network access, reducing attack surfaces. It supports MFA and SSO via SAML IdPs, enabling seamless integration.

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.

ZIA's advanced SWG inspects traffic at the cloud edge, protecting users from malware, malicious URLs, and phishing. It leverages AI-driven analysis, real-time URL filtering, and full SSL inspection to block ransomware and enforce acceptable use policies without degrading user experience. ZIA secures all users and devices. Integrated with ZPA, Zscaler delivers DLP and browser isolation, securing sensitive data across web, email, apps & BYOD, 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.

ZIA's FWaaS delivers consistent policies across locations and devices via a centralized, cloud-native platform. It provides advanced security controls, including network segmentation, access control, intrusion detection/prevention, and Layer 7 (L7) application-aware policy enforcement. With centralized management, real-time traffic visibility, and deep packet inspection, ZIA simplifies operations while enhancing security across all ports and protocols.

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.

Zscaler offers real-time analytics with custom dashboards for cloud usage, integrating seamlessly with SIEM for data streaming. The solution provides end-to-end NetFlow traceability and real-time user experience monitoring to detect traffic patterns and bottlenecks from user to application. Zscaler also captures raw logs and provides in-depth analytics for insights into network performance, security threats, and user behavior across distributed environments.

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.

Zscaler integrates proprietary and third-party CTI feeds from 40+ sources, continuously updated by Zscaler's threat research teams. Using advanced threat intelligence and automated malware analysis, Zscaler's Single Scan Multi Action engine and Sandbox detect and block malicious traffic in near real time, correlating user activity and network behavior with known threats. Our UVM further enhances security, leveraging ML models and integrating 3rd party sources.

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.

Zscaler integrates multi-mode CASB to provide visibility and control over cloud apps, securing data across SaaS platforms. It offers AI-driven data discovery, Shadow IT visibility, automated controls, and extended DLP for SaaS, email, endpoints, and private apps. API-based integration with 20+ apps enables DLP, malware scanning, and SaaS Security Posture Management. Our CASB integrates with Bitglass and MCAS and integrates with tools like ServiceNow for orchestration.

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.

Zscaler commits to SLAs with defined service credits and clear performance metrics, ensuring accountability in availability, latency, and security. Specific SLAs include:

- Global Availability: >= 99.999%
- Global Latency: <= 100ms

Zscaler's SLAs cover latency without exclusions for DLP or malware scanning. Violations are subject to penalties as detailed in each product's SLA sheet, available at: http://www.zscaler.com/legal/sla-support. For transparency, we provide reporting on proxy latency and offer a real-time public status page for cloud availability at https://trust.zscaler.com. Full Details listed at: https://www.zscaler.com/legal/sla-support

Zscaler's services are governed by our End User Subscription Agreement, available at https://www.zscaler.com/legal/end-user-subscription-agreement. While we operate as a multi-tenant cloud provider with standard terms, Zscaler is open to negotiating mutually agreeable terms and conditions upon selection as a vendor.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L11 – Service Category 11: Governance, Risk, and Compliance (GRC)

Respondent Name: Hayes e-Government Resources

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Hayes e-Government Resources

Solution Name: Critical Start - Vulnerability Management Services

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.

Critical Start's Vulnerability Management Service is a fully managed service that enables security leaders to effectively run a vulnerability management program by offloading burdensome operational tasks. VMS delivers turnkey managed vulnerability scanning, expert Vulnerability Prioritization, and rich, multi-level reporting. Stakeholders can leverage expert guidance to make sound, data-driven remediation decisions that reduce risk to the organization, all without overextending internal teams or budgets The managed service leverages Critical Start's partnership with Qualys utilizing their industry leading end-to-end vulnerability management, detection, and response solution, Qualys VMDR.

Critical Start's managed services engineers provide operational execution of vulnerability scanning, ongoing operational monitoring, and detailed reporting, all of which contribute to a comprehensive view of an organization's exposure landscape. All findings provided through rich, contextualized VMS dashboards and reports are based on expert analysis of vulnerabilities and potential exposures in the customer environment. Customers receive concise directions and prescriptive patching guidance for effective and efficient vulnerability management that help them reduce cyber risk and minimize their 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.

Critical Start's VMS is built on top of Qualys VMDR and Critical Start can provide the licenses. The service combines the use of agents for remote devices as well as network scanners. Customers can choose from self-managed scans conducted in-house, or fully managed scans executed by experts in the Critical Start RSOC. Critical Start provides a definitive list of patch recommendations derived from internal and external analysis to identify exactly how to remediate.

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.

Prioritization is critical when you have high volumes of vulnerabilities and limited time for remediation. Critical Start's VMS prioritizes vulnerabilities based on crucial factors, including weaponization, exploitability, and asset criticality. Critical Start correlates the findings from VM solution with a competitive up-to-date thread feed and helps customers prioritize the vulnerabilities based on the risk they pose.

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.

As Critical Start leverages Qualys VMDR for scanning, integration with Service Now is available and includes the ability to automate ticket creation, assignment to rightful owners and closure upon remediation.

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.

Critical Start's VMS includes customizable vulnerability and remediation reports and dashboards, with dozens of available metrics to help organizations measure and articulate the performance of their vulnerability management program. Additionally, the VMS Dashboard Toolkit offers timely views of critical vulnerability intelligence

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.

As Critical Start's VMS service leverages the Qualys VMDR platform, we give clients full access to the Qualys portal as well as reporting in our CORR portal. Critical Start will configure and provide up to ten (10) custom dashboards within the Qualys platform to provide details for vuln counts, time to remedaition, patch compliance rates and more.

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.

Critical Start's VMS service provides a Prescriptive Patch Catalog which identifies the definitive list of patch recommendations to remediate identified vulnerabilities. Reports and outputs from these lists can be incorporated into various patch management 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.

Critical Start's VMS includes our Vulnerability Prioritzation service which incoproprates information from our Cyber Threat Intelligence team to help identify weaponized vulnerabilities, active campains and availability/ease of exploit code being distributed in the wild. We pair this with CVE scores and asset criticalilty to help teams prioritze remediation efforts in a risk based context.

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

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Hayes e-Government Resources

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.

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Hayes e-Government Resources

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 organizations address 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:

Service Level Agreement for Hosted Services This Service Level Agreement ("SLA") between Tenable ("Tenable") and Customer is subject to the applicable license or subscription agreement between Tenable and Customer under which the Customer licenses the Hosted Services, or if the parties have not executed such separate agreement, the Tenable Master Agreement located at http://static.tenable.com/prod_docs/tenable_slas.html (the "Agreement"). All defined terms used in this SLA and not defined herein shall have the meaning assigned to them in the Agreement. Tenable shall provide the Hosted Services and Software in connection with the Agreement. This SLA governs Tenable's performance and delivery of the Hosted Services to Customer.

1. Definitions.

"Potential Uptime" means the amount of time in a given month. "Production Uptime" represents the amount of time in a given month that Customer has the ability to log in or access the Hosted Services user interface (or authenticate to APIs) and perform associated Scanning related activity. Potential Uptime is measured by Tenable in a given month by the following calculation: Production Uptime = (Potential Uptime – Hosted Services Interruption Time) / (Potential Uptime – Exclusions) "Hosted Services Interruption Time" is the period of time for which the Hosted Services (or any material portion thereof) are unavailable due to issues caused by or attributable to Tenable or its agents. Hosted Services Interruption Time does not include Regular Maintenance or Scheduled Maintenance. "Regular Maintenance" is the period of time under which the Hosted Services may be unavailable for recurring maintenance work. Tenable attempts to schedule this time when usage of the Hosted Services is light across Tenable's customer base and therefore, Tenable shall use commercially reasonable efforts to only conduct Regular Maintenance daily between the hours of 7AM and 9AM (ET) and non-business days. Regular Maintenance is required in order to update Tenable's plug-in databases as well as to maintain system health requirements. Tenable shall use commercially reasonable efforts to minimize any Regular Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Regular Maintenance. "Scheduled Maintenance" is the period of time under which the Hosted Services may be unavailable for non-recurring maintenance. Scheduled Maintenance is required in order to provide updates to the Hosted Services as well as to maintain system health requirements. Tenable shall provide Customer at least twelve (12) hours advance notice prior to Scheduled Maintenance; provided, however, Tenable shall endeavor to provide at least twenty-four (24) hours advanced notice for Scheduled Maintenance. Notice for Scheduled Maintenance will be provided at the following URL or successor location: status.tenable.com. Tenable shall use commercially reasonable efforts to minimize any Scheduled Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Often times, Customer will not experience any Hosted Services Interruption Time during periods of Scheduled Maintenance. "Emergency Maintenance" describes maintenance for certain emergency situations, where

advance notice may be not be feasible, possible or practical. Tenable shall use commercially reasonable efforts to minimize any Emergency Maintenance windows to the minimum time necessary to support performance of the Hosted Services. Periods of Emergency Maintenance shall be included in Hosted Services Interruption Time. Tenable Confidential and Proprietary SLA v.3

2. Service Levels Commitment. Tenable commits to provide a 99.95% Production Uptime with respect to the Hosted Services during each calendar month of the subscription term.

3. Service Level Credits. If Tenable fails to perform the Hosted Services in accordance with the Service Level Commitment, then Customer may request a Service Level Credit in accordance with this SLA. Service Level Credits shall be Customer's sole and exclusive remedy for unavailability or performance degradation of the specific Hosted Services.

4. Weighting Factor. The "Weighting Factor" for calculation of the Service Level Credit is set forth below and correlates to the relative unavailability of the Hosted Service in a given month.

Production Uptime between 99.95% and 100% = 0 Production Uptime between 95.00% and 99.94% = .1 Production Uptime between 90.00% and 94.99% = .15 Production Uptime below 90% = .2

5. Calculation of Service Level Credits. The following equation shall be used to calculate any Service Level Credits: Service Level Credit (in $) = Weighting Factor multiplied by the monthly fee for applicable Hosted Service.

Example: Production Uptime in a given month is 95%. The monthly fee for the Hosted Service is $100 (Annual fee for the Hosted Services is $1,200). Service Level Credit (in $) = (0.1) x $100 = $10.

If Customer has paid in advance for one or more years of the Hosted Services, monthly fees will be calculated on a pro rata basis.

6. Exclusions. "Exclusions" shall mean any time for which the Hosted Services are unavailable to do any of the following: (i) Customer's breach of, or failure to perform any obligations under, this SLA or the Agreement; (ii) issues relating to Customer's environment, internal networks, computer systems, firewalls or Customer's inability to connect to the internet; (iii) Force Majeure Events; or (iv) issues arising from failures, acts or omissions Tenable's upstream service providers (i.e. AWS).

7. Requests. In order to receive a Service Level Credit, Customer must request such by emailing Tenable at credits@tenable.com, within 10 days of the end of the applicable month. If Customer is past due or in default with respect to any payment or any material contractual obligations to Tenable, Customer is not eligible for any Service Level Credit. Service Level Credits are non-refundable and may only be applied to future upgrades or renewals of the specific Tenable Hosted Services affected.

8. Changes. This Service Level Commitment may be amended by Tenable in its reasonable discretion but only after providing thirty (30) days' advance notice. Tenable may provide such notice either as a note on the screen presented upon logging in to the Hosted Services, by posting updated terms on Tenable's website, or by email to the email addressed registered with Customer's account. This SLA was updated on October, 2023 (ver 3).

Master Agreement, accepted via a click-thru acknowledgement at time of installation:

Due to the document exceeding the allotted character limit, the full documentation can be located at https://static.tenable.com/prod_docs/Tenable-Master-Agreement-Template-v6-(2.2023)-CLICK.pdf . We have included what we can below.

TENABLE MASTER AGREEMENT This Master Agreement (this "Agreement") is made by and between Tenable (as defined below) and the customer licensing Products and/or receiving services ("Customer") with an effective date as of the date Customer clicks to accept this Agreement (the "Effective Date"). Hereinafter, each of Tenable and Customer may be referred to collectively as the "Parties" or individually as a "Party".

1. Definitions. (a) "Affiliate" means any entity that controls, is controlled by, or is under common control with a Party. "Control" shall mean: (1) ownership (either directly or indirectly) of greater than fifty percent (50%) of the voting equity or other controlling equity of another entity; or (2) power of one entity to direct the management or policies of another entity, by contract or otherwise. (b) "Documentation" means the then-current official user manuals and/or documentation for the Products available at docs.tenable.com (or a successor location). (c) "Hosted Services" are a type of service offered through Tenable's cloud-based software as a service (SaaS) platform and include Scans and access to and use of the hosted environment (the "Hosted Environment"). (d) "Product(s)" means any of the products that Tenable offers, including Software, Hosted Services, Hardware (if any), Support Services and Professional Services. (e) "Professional Services" means services purchased, including consulting services which are relevant to the implementation and configurations of Tenable Products as well as on-site or virtual training courses. Generally, Professional Services are defined either in a separate SOW or a Services Brief. Professional Services do not include the Hosted Services or Support Services. (f) "Scan(s)" are a function performed by the Software and/or the Hosted Services on Scan Targets, which are conducted in order to provide data to Customer regarding its network security. "PCI Scans" are a specific type of Scan designed to assess compliance with the Payment Card Industry Data Security Standard. "Scan Data" is the resulting information created by the Scan. "Scan Target(s)" are the targets or subjects of a Scan. (g) "Services Brief" means the document which outlines Tenable's basic, pre-packaged installation or training Professional Services offered under a Tenable SKU and which do not require a separate SOW. Current versions of Services Briefs may be found at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). For the avoidance of doubt, Customer may purchase commercial off the shelf SKU-based Professional Services without executing a separate Statement of Work. A "SOW" or "Statement of Work" shall further describe Professional Services, the terms of which may be customized and which shall require execution by the Customer. (h) "Software" means each software product made available by Tenable under this Agreement for download. Software includes patches, updates, improvements, additions, enhancements and other modifications or revised versions of the same that may be provided to Customer by Tenable from time to time. (i) "Technical Data" means data Customer uploads or runs through or on the Products, or is otherwise generated thereby, including information regarding licensing metrics and product behavioral data. (j) "Tenable" means: (i) Tenable, Inc., if Customer is a commercial entity or individual located in North or South America (Tenable, Inc. is a Delaware corporation having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); (ii) Tenable 2 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 Public Sector LLC, if Customer is an agency or instrumentality of the United States Government, a commercial entity operating predominantly as a federal systems integrator

for eventual sale or resale or for the benefit of the United States Government, or an agency or instrumentality of a State or local government within the United States (Tenable Public Sector LLC is a Delaware limited liability company having offices at 6100 Merriweather Drive, 12th Floor, Columbia, MD 21044); or (iii) Tenable Network Security Ireland Limited, if Customer is located outside of North or South America (Tenable Network Security Ireland Limited is a private limited company having offices at 81b Campshires, Sir John Rogerson's Quay, Dublin 2, Ireland).

2. Orders and Transactions. (a) Reseller Transactions. If Customer purchases Tenable Products through an authorized Tenable reseller (a "Reseller"), all terms related to pricing, billing, invoicing and payment ("Payment Terms") set forth in this Agreement (if any) shall not apply. For the avoidance of doubt, all such Payment Terms shall be as agreed to between Customer and Reseller. To place an order, Customer shall provide the Reseller with a purchase order (or other similar document acceptable to Reseller) in response to a valid quote from such Reseller. Following Reseller's receipt of such purchase order, Tenable shall issue a sales order confirmation or other similar order acceptance document (the "Ordering Document"). No order shall be deemed accepted by Tenable until Tenable issues the Ordering Document. The Ordering Document shall set forth all Products (and corresponding licensing metrics) purchased by Customer. (b) Direct Transactions. If the Parties have agreed to transact directly, the following Payment Terms shall apply. Customer agrees to pay all amounts due as specified in a Tenable invoice. Fees for Hosted Services are charged for access to the Host Environment (as defined herein), not actual usage. Payment is due within thirty (30) days from the date of Tenable's invoice to Customer. Customer will pay directly or reimburse Tenable for any taxes (including, sales or excise taxes, value added taxes, gross receipt taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, imposed on or arising out of this Agreement. Notwithstanding the foregoing, Tenable will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. Customer agrees to pay Tenable without deducting any present or future taxes, withholdings or other charges except those deductions it is legally required to make. If Customer is legally required to make any deductions or withholding, Customer agrees to provide evidence of such withholding upon request. If a certificate of exemption or similar document or proceeding is necessary in order to exempt any transaction from a tax, Customer shall provide such certificate or document to Tenable. (c) Delivery and Installation. Delivery of Tenable Products ("Delivery") shall be deemed to occur on the date of availability for electronic download or electronic access. Tenable has no duty to provide installation services for Tenable Products unless installation services are purchased separately.

3. Term and Termination. (a) Agreement Term. This Agreement shall commence upon the Effective Date and continue until terminated in accordance with the terms set forth herein. (b) License Term and Renewals. The "License Term" is the term of the license or subscription for Products as set forth in the Ordering Document. If this Agreement has been signed by both Parties, then unless otherwise agreed to in writing, any License Term, including renewals, shall be governed by the terms set forth herein. If this Agreement has been accepted via shrinkwrap or click through, upon any renewal of the License Term, the terms then available at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location) will govern such renewal. Customer agrees that use of the Products at the time of such renewal will be deemed full and adequate acceptance of the updated terms. (c) Termination for Cause. Either Party may terminate this Agreement for cause if the other Party materially breaches this Agreement provided that such breaching Party has received written notice of such breach and failed to cure such breach within thirty (30) days. If this Agreement is terminated for cause by either Party, Customer

shall remove all copies of the Products from any Customer systems and cease to use any Software or Hosted Services purchased hereunder. Further, Customer shall certify to Tenable that it has returned or destroyed all copies of the Software. If this Agreement is terminated for cause by Tenable, Customer shall remain responsible for any outstanding payment obligations throughout the rest of the License Term. (d) Termination for Convenience. Customer may terminate this Agreement for any lawful reason upon ninety (90) days' prior written notice to Tenable. If Customer terminates for convenience, Customer shall not receive a refund and shall remain obligated to pay for Products for which it has previously entered into a transaction as well as any additional payment obligations agreed upon prior to the termination date.

4. Products. (a) Product-Specific Terms. Pursuant to this Agreement, Customer may receive the right to use various Products as further described in the attached schedules (each, a "Schedule"). Terms related to Customer's use of Software are described in Schedule A 3 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 (Software). Terms related to Customer's use of Hosted Services are described in Schedule B (Hosted Services). Terms related to the provision of Professional Services are described in Schedule C (Professional Services). For each Product, Customer will have the right to use the corresponding Documentation. (b) Licensing Model. Product licenses shall be in accordance with the terms of the applicable licensing model as set forth in the Documentation and/or the Ordering Document, which may include limitations on Scan Targets, compute, storage, resource utilization, License Term, the number of users, seats, licenses and/or types of modules licensed. Product licenses shall commence upon Delivery and shall be either perpetual or subscription in nature. Tenable shall use commercially reasonable efforts to meter resource utilization and assess likeness or uniqueness of Scan Targets within each Product/module licensed. If Customer exceeds the license restrictions, Customer must purchase an upgraded license to allow for all actual or additional usage, and Tenable or its Reseller may promptly invoice Customer for any such overages at a price not to exceed Tenable's then-current rates. Discrepancies in Scan Target or utilization count is the sole responsibility of the Customer to resolve. (c) Restrictions on Use. Customer shall not directly or indirectly: (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive, obtain or modify the source code of the Products; (ii) reproduce, modify, translate or create derivative works of all or any part of the Products; (iii) remove, alter or obscure any proprietary notice, labels, or marks on the Products; (iv) without Tenable's prior written consent, use the Products in a service bureau, application service provider or similar capacity; (v) without signing Tenable's Managed Security Services Provider Addendum, use the Products to provide any managed service to a third party; (vi) use the Products in order to create competitive analysis or a competitive product or service; (vii) copy any ideas, features, functions or graphics in the Product; or (viii) without Tenable's prior written consent, interfere with or disrupt performance of Hosted Services (e.g., perform penetration testing on Tenable systems). Customer may only use the Products to manage or gather information from Scan Targets owned or hosted by Customer or its Affiliates, or third parties for which Customer has received express authorization to Scan. (d) Intellectual Property in Products. This Agreement does not transfer to Customer any title to or any ownership right or interest in the Products. Any rights in the Products not expressly granted in this Agreement are reserved by Tenable. If Customer provides Tenable with any comments, suggestions, or other feedback regarding the Product, Customer hereby assigns to Tenable all right, title and interest in and to such feedback. For clarity, such feedback shall not contain Customer Confidential Information and shall not reference or identify Customer or its users. (e) Customer Requirements. In order to use the Products, Customer must meet or exceed the specifications found in the

Documentation. (f) Product Features. Customer agrees that purchase of any Product is not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Tenable regarding future functionality or features. Tenable reserves the right to withdraw features from future versions of the Products provided that: (i) the core functionality of the affected Product remains the same; or (ii) Customer is offered access to a product or service providing materially similar functionality as the functionality removed from the affected Product. The preceding remedies under this Section 4(f) are the sole remedies available if Tenable withdraws features from the Products. (g) Rights Granted to Tenable. Provided that Tenable shall not publicly disclose any Customer Confidential Information, Tenable may: (i) use Technical Data for reasonable business purposes, including Support Services, license validation, research and development, feature creation, and Product testing; (ii) include aggregated and anonymized Technical Data in public materials; and (iii) retain Technical Data which is anonymized after the termination of this Agreement. (h) Hardware. Any Hardware purchased under this Agreement (if any) will be subject to the terms and conditions of Schedule D located at http://static.tenable.com/prod_docs/tenable_slas.html (or a successor location). (i) Temporary Limitation. If Tenable reasonably believes: (i) Customer's use of the Products places an unreasonable or disproportionate burden on the Products; (ii) Customer's use of the Products poses a risk or threat to the Products (including any systems supporting the Products), Tenable, or a third party; or (iii) Customer's usage exceeds the limitations of the license, then Tenable may temporarily limit Customer's access to or use of the Products or any specific feature therein. Tenable may also suspend or limit access to the Products if Customer fails to make any payments related to this Agreement. Tenable will, to the extent practical under the circumstances, use commercially reasonable efforts to provide Customer with prior written notice of any such limitation (email or in product messaging shall be sufficient). When commercially reasonable, Tenable shall promptly restore access once the Customer has remediated the issue. For the avoidance of doubt, Customer is responsible for all normal fees during any period for which usage or access is limited pursuant to this section. (j) Additional Details on Use Restrictions for Tenable Security Network Ireland Limited. The following shall only apply for transactions with Tenable Security Network Ireland Limited. Notwithstanding anything in Section 4(c), decompiling the Product is 4 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 permitted to the extent the laws of Customer's jurisdiction give Customer the right to do so to obtain information necessary to render the Products interoperable with other software; provided, however, that Customer must first request such information from Tenable and Tenable may, in its discretion, either provide such information to Customer or impose reasonable conditions, including a reasonable fee, on such use of the Products to ensure that its proprietary rights in the Product are protected.

5. Support. (a) Support Services. Tenable shall provide Customer with support services (the "Support Services") in accordance with Tenable's then-current Technical Support Plans (available at http://static.tenable.com/prod_docs/tenable_slas.html or a successor location) and consistent with Tenable's End of Life and End of Sale definitions contained therein. The Support Services include bug fixes, updates (including new vulnerability plug-ins), or enhancements that Tenable makes generally available to users of the Products. The Support Services also include the provision of new minor (Example: 1.1.x to 1.2.x, etc.) and major version releases of the Products (Example: 1.x to 2.x, etc.). (b) Support Fees. Standard Support Services for Products licensed for a finite License Term will be provided at no additional charge beyond the license fee for the duration of the License Term. Support Services for Products licensed on a perpetual basis must

be purchased separately in advance. In all cases, premium support may be purchased at an additional charge. If during the course of a perpetual license Customer terminates or fails to renew the Support Services, Customer may, at any time during the term of this Agreement, request that Tenable reinstate the Support Services provided that Customer pays for the lapsed Support Services in an amount equal to the total fees Customer would have paid for the Support Services between the time Customer's Support Services lapsed and the then-current date.

6. Confidentiality. (a) Definition. "Confidential Information" means information learned or disclosed by a Party under this Agreement that should reasonably be assumed to be confidential or proprietary, including the Products and the terms of this Agreement. Confidential Information will remain the property of the disclosing Party, and the receiving Party will not be deemed by virtue of this Agreement or any access to the Confidential Information to have acquired any right, title or interest in or to the Confidential Information. (b) Obligations. Each Party agrees to only use the Confidential Information in connection with this Agreement or a purchase hereunder. The receiving Party agrees to hold the disclosing Party's Confidential Information confidential using at least the same level of protection against unauthorized disclosure or use as the receiving Party normally uses to protect its own information of a similar character, but in no event less than a reasonable degree of care. Each Party may share Confidential Information with its Affiliates or authorized contractors in the performance of its duties under this Agreement; provided, however, that each Party shall be responsible to ensure that such Affiliate or authorized contractors are bound by obligations of confidentiality at least as stringent as those set forth in this Agreement. (c) Exclusions. Confidential Information shall not include information that: (i) is already known to the receiving Party free of any confidentiality obligation; (ii) is or becomes publicly known through no wrongful act of the receiving Party; (iii) is rightfully received by the receiving Party from a third party without any restriction or confidentiality; or (iv) is independently developed by the receiving Party without reference to the Confidential Information. Confidential Information does not include Scan Data that has been aggregated or anonymized so that it is not attributable to the disclosing Party. If Customer requests or performs scans on third party Scan Targets, and such third party inquires with Tenable about the scan, Tenable shall inform Customer and allow Customer to resolve any disputes with the third party. If Customer fails to contact the third party, Customer agrees that Tenable may provide Customer's business contact information to the owner of the Scan Targets as well as to relevant authorities, and such disclosure shall not be considered a breach of confidentiality. (d) Sensitive Information. The Parties agree that Customer's disclosure of sensitive, personal information (e.g., social security numbers, national identity card numbers, personal credit card information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and health care data) ("Sensitive Information") is not required for Tenable to perform its duties under this Agreement or sell any Products hereunder. If Customer inadvertently or unintentionally discloses any Sensitive Information to Tenable, Customer shall identify to Tenable that it has disclosed Sensitive Information and Tenable shall promptly return and/or destroy such Sensitive Information. (e) Legal Disclosures; Remedies. The receiving Party may disclose Confidential Information if required to do so by law provided the receiving Party shall promptly notify the disclosing Party so that the disclosing Party may seek any appropriate protective order and/or take any other action to prevent or limit such disclosure. If required hereunder, the receiving Party shall furnish only that portion of the Confidential Information disclosure of which is legally required. The receiving Party acknowledges and agrees that the breach of any term, covenant or provision of this Agreement may cause irreparable harm to the disclosing Party and, accordingly, upon the threatened or

actual breach by the receiving Party of any term, covenant or provision of this Agreement, the disclosing Party shall 5 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 be entitled to seek injunctive relief, together with any other remedy available at law or in equity. The receiving Party will notify the disclosing Party promptly of any unauthorized use or disclosure of the disclosing Party's Confidential Information.

7. Representations and Warranties; Disclaimer. (a) Warranty of Authority. The Parties hereby represent and warrant that they have the full power and authority to enter into this Agreement. (b) Products. Product warranties and associated warranty periods are set forth in the relevant Schedules. (c) Antivirus Warranty. Tenable represents it has taken commercially reasonable efforts to ensure that the Products, at the time of Delivery, are free from any known and undisclosed virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that would erase data or programming or otherwise cause the Products to become inoperable or incapable of being used in the manner for which it was designed or in accordance with the Documentation. (d) Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT AND TO THE GREATEST EXTENT PERMITTED BY LAW, TENABLE OFFERS ITS PRODUCTS "AS-IS" AND MAKES NO OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY WARRANTIES OF TITLE, NON INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SECURITY, INTEGRATION, PERFORMANCE AND ACCURACY, AND ANY IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. THE WARRANTIES SET FORTH IN THIS AGREEMENT ARE MADE TO CUSTOMER FOR CUSTOMER'S BENEFIT ONLY. CUSTOMER'S USE OF THE PRODUCTS IS AT CUSTOMER'S OWN RISK. CUSTOMER UNDERSTANDS THAT ASSESSING NETWORK SECURITY IS A COMPLEX PROCEDURE, AND TENABLE DOES NOT GUARANTEE THAT THE RESULTS OF THE PRODUCTS WILL BE ERROR-FREE OR PROVIDE A COMPLETE AND ACCURATE PICTURE OF CUSTOMER'S SECURITY FLAWS, AND CUSTOMER AGREES NOT TO RELY SOLELY ON SUCH PRODUCTS IN DEVELOPING ITS SECURITY STRATEGY. CUSTOMER ACKNOWLEDGES THAT THE PRODUCTS MAY RESULT IN LOSS OF SERVICE OR HAVE OTHER IMPACTS TO NETWORKS, ASSETS OR COMPUTERS (INCLUDING MODIFICATION OF SCAN TARGETS), AND CUSTOMER IS SOLELY RESPONSIBLE FOR ANY DAMAGES RELATING TO SUCH LOSS OR IMPACT.

8. Limitation of Liability. (a) Direct Damages. The cumulative liability of one Party to the other for all claims arising from or relating to the Products or this Agreement (including without limitation, any cause of action sounding in contract, tort or strict liability) shall be limited to proven direct damages in an amount not to exceed, in the aggregate, the fees paid by Customer for the Products over the twelve (12) months immediately prior to the event giving rise to the claim. (b) Indirect Damages. Neither Party shall be liable to the other for any indirect, incidental, special, punitive, consequential or exemplary damages regardless of the nature of the claim. This prohibition on indirect damages shall include, but not be limited to, claims based on lost profits, cost of delay, any failure of Delivery, business interruption, cost of lost or damaged data, or liabilities to any third parties even if such Party is advised of the possibility thereof. (c) Carve Outs. The liability caps set forth in Sections 8(a) and 8(b) shall not apply to damages resulting from: (i) personal injury or death; (ii) fraud or willful misconduct; (iii) indemnification obligations set forth in Section 9 (Indemnification); or (iv) Customer's breach of Section 4(c) (Restrictions on Use). (d) Limitations; Time Period. Each of the limitations set forth in this Section 8 shall be enforced to the

fullest extent of the law. Any laws preventing such limitations shall only apply to the extent required by law and the remaining unaffected terms shall apply in full. Unless expressly prohibited by law, each Party shall have a period of no greater than twelve (12) months from the date the cause of action accrues to bring a claim against the other Party for such cause of action.

9. Indemnification. (a) Indemnification Obligations. (i) By Tenable. Tenable shall (at its sole cost and expense): (i) defend and/or settle on behalf of Customer (including Customer's officers, directors, employees, representatives and agents); and (ii) indemnify Customer for, any third party claims brought 6 Tenable Confidential and Proprietary Tenable Master Agreement v.6 2.2023 against Customer based upon a claim that Customer's use of the Products in accordance with this Agreement infringes or misappropriates such third party's intellectual property rights in a jurisdiction which is signatory to the Berne Convention. (ii) By Customer. Customer shall (at its sole cost and expense): (i) defend and/or settle on behalf of Tenable (including Tenable's officers, directors, employees, representatives and agents) and (ii) indemnify Tenable for, any third party claims brought against Tenable arising out of or relating to Customer's use of the Products to perform Scans on third party Scan Targets, except to the extent that any such claim or action is caused by a failure of the Products to materially comply with the Documentation. (b) In Case of Infringement. If Customer's use of the Products is, or in Tenable's opinion is likely to be, the subject of an infringement claim, Tenable may, in its sole discretion and expense: (i) modify or replace the infringing Products as necessary to avoid infringement, provided that the replacement Products are substantially similar in functionality; (ii) procure the right for Customer to continue using the infringing Products; or (iii) terminate this Agreement and, upon Customer's return or certified destruction of the infringing Product, provide Customer a pro-rata refund calculated as follows: (x) for infringing Products licensed on a subscription basis, the refund shall consist of any prepaid but unused fees for the remainder of the applicable License Term; or (y) for infringing Software licensed on a perpetual basis or infringing Hardware, the refund shall consist of a straight line depreciation of the license fee based on a three (3) year useful life as well as any prepaid but unused fees for separately charged Support Services. This Section 9 sets forth Tenable's sole and exclusive liability and Customer's sole and exclusive remedy with respect to any claim of intellectual property infringement. (c) Exclusions. Tenable shall have no liability with respect to a third party intellectual property infringement claim arising out of: (i) modifications of the Product made by Customer or a party under its control to conform with Customer's specifications; (ii) modifications of the Product made by anyone other than Tenable or a Tenable authorized third party; (iii) Customer's use of the Product in combination with other products or services not provided by Tenable; (iv) Customer's failure to use any updated versions of the Product made available by Tenable; or (v) Customer's use of the Product in a manner not permitted by this Agreement or otherwise not in accordance with the Documentation. (d) Requirements. The indemnitor shall only be responsible for the indemnification obligations set forth in this Section 9 if the indemnitee: (i) provides the indemnitor prompt written notice of such action or claim; (ii) gives the indemnitor the right to control and direct the investigation, defense, and/or settlement of such action or claim; (iii) reasonably cooperates with the indemnitor in the defense of such a claim (at the indemnitor's expense); and (iv) is not in breach of this Agreement. Nothing herein shall prevent the indemnitee from engaging in defense of any such claim with its own legal representation, provided that this does not materially prejudice the indemnitor's defense. The indemnitor may not settle any claim on behalf of the indemnitee without obtaining the indemnitee's prior written consent; provided, however, the indemnitor shall not be required to obtain consent to

settle a claim which settlement consists solely of: (x) discontinued use of infringing Products and/or (y) the payment of money for which the indemnitor has a duty to indemnify.

10. Legal Compliance. (a) Generally. The Products are intended solely for lawful purposes and use. Both Parties, and their agents and Affiliates, agree to perform their respective obligations in an ethical manner that complies with all applicable national, federal, state and local laws, statutes, ordinances, regulations and codes ("Applicable Laws") including, without limitation, the Computer Fraud and Abuse Act (CFAA), 18 USC Sec. 1030, the U.S. Foreign Corrupt Practices Act of 1977, as amended, and the UK Bribery Act of 2010. If Customer violates this Section 10, Tenable may terminate this Agreement immediately. (b) Trade Controls. Applicable Laws include U.S. export laws (including the International Traffic in Arms Regulation (ITAR), 22 CFR 120-130, and the Export Administration Regulation (EAR), 15 CFR Parts 730 et seq.) and the anti-boycott rules implemented by the Departments of Commerce and Treasury. Information regarding export classifications of Tenable's Products may be found on its website (www.tenable.com/export-controls or a successor location). Customer agrees that it will be the exporter of record any time it causes the Products to be accessed outside the United States or by a national of any country other than the United States. The Parties further agree to comply with trade and economic sanctions, rules, and regulations of the United States, European Union, EU member states, United Kingdom and other applicable government authorities and shall not engage in prohibited trade to persons or entities who are the subject of an active sanction, embargo, or executive order. Customer hereby acknowledges and confirms that Customer (including Customer's officers, directors, employees, representatives and agents): (i) is not included on, owned or controlled by an individual or entity included on, or acting on behalf of an individual or entity included on any of the restricted party lists maintained by the U.S. Government (e.g., Specially Designated Nationals List, Foreign Sanctions Evader List, Sectoral Sanctions Identification List, Denied Persons List, Unverified List, Entity List or List of Statutorily Debarred Parties) (collectively, "Restricted Parties"); (ii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use by or for Restricted Parties; (iii) will not export, re-export, transfer, re-transfer or otherwise ship, directly or indirectly, the Products or related technology to or for use in, by or for countries or territories subject to U.S. economic sanctions (e.g., Crimea, Cuba, Iran, North Korea, or Syria); or (iv) will not use or sell the Products…

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L13 – Service Category 13: Vulnerability Assessment and Management

Respondent Name: Hayes e-Government Resources

Solution Name: Zscaler - Unified 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.

Zscaler's Next-Gen Unified Vulnerability Management (UVM) solution enhances the capabilities of existing vulnerability scanners, such as Tenable and Qualys, by scanning assets for vulnerabilities and ingesting data from these scanners. It prioritizes vulnerabilities using customizable risk scoring tailored to the organization's needs. The solution can also automate remediation workflows through integrations with tools like ServiceNow and JIRA.

Zscaler's UVM enriches vulnerability data and threat intelligence feeds with additional findings and business context, including asset details, mitigating controls, and user behavior. Leveraging the Zscaler's Data Fabric for Security, it curates and correlates data from hundreds of sources, in any format and scale. The UVM module aggregates risk factors, mitigating controls, and business context, enabling organizations to understand their risk in a comprehensive and holistic manner for the first time.

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.

Our solution will ingest the scan data from different toolsets already present in the organization and present a prioritized view of the vulnerabilities. On its own, UVM does not scan endpoints,servers,network devices and applications.

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.

Zscaler ingests scan data from existing toolsets and uses contextual asset data to prioritize vulnerabilities for remediation. It offers out-of-the-box multi-factor risk scores with mitigating controls and industry best practices, plus custom risk factors. EPSS is included by default, and scoring adjusts for specific risk factors and controls, providing a prioritized list tailored to the organization's unique environment and risk profile.

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.

Zscaler's UVM has bi-directional integration with tools like ServiceNow and JIRA. Ticket creation and assignment to address vulnerabilities can be automated as well as the progress tracked.

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.

A customized reports feature is available within the solution that can be used to build reports on the assets, findings, risk scores, vulnerability descriptions and recommended fixes.

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.

Zscaler's UVM provides an out of the box remediation tracking dashboard. Additionally, custom dashboards can be created as well to track other metrics such as security posture, open vulnerabilities, and patch-compliance.

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.

Zscaler integrates with patch management systems such as SCCM to kick off a remediation notification workflow, which SCCM can then in turn, can then deploy patches to the vulnerable systems.

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.

Our solution pulls in open source feeds to provide CISA KEV and EPSS. The tool also leverages custom threat intel sources to provide additional insights. The data can be augmented by bringing in threat intel data from 3rd party sources.

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.

Full Details listed at: https://www.zscaler.com/legal/sla-support

Zscaler's services are governed by our End User Subscription Agreement, available at https://www.zscaler.com/legal/end-user-subscription-agreement. While we operate as a multi-tenant cloud provider with standard terms, Zscaler is open to negotiating mutually agreeable terms and conditions upon selection as a vendor.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L14 – Service Category 14: Cybersecurity Threat Intelligence (CTI)

Respondent Name: Hayes e-Government Resources

Solution Name: Palo Alto Networks - Coretx 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.

Cortex 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.

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L14 – Service Category 14: Cybersecurity Threat Intelligence (CTI)

Respondent Name: Hayes e-Government Resources

Solution Name: Splunk - Threat Intelligence 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 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.

Splunk Enterprise Security (ES) and Threat Intelligence Management (TIM) solution aggregates threat data from diverse sources, including commercial feeds, open-source intelligence, and internal telemetry, to provide a comprehensive view of the threat landscape. By leveraging Splunk's data analytics and machine learning capabilities, the platform continuously analyzes this data to uncover emerging threats, track trends, and detect indicators of compromise (IoCs). This proactive analysis provides actionable intelligence that supports both immediate threat detection and long-term strategic defense.

Splunk integrates CTI into existing security operations workflows seamlessly, enhancing an organization's detection, prevention, and response efforts. Through correlation of CTI data with internal events, Splunk prioritizes alerts based on risk, allowing security teams to focus on the most significant threats and reduce alert fatigue. Its adaptive dashboards and customizable visualizations offer security teams intuitive views of threat activity and emerging risks, enabling rapid assessment and decision-making.

Splunk supports Security Orchestration, Automation, and Response (SOAR) capabilities, allowing for automated workflows that incorporate CTI data into incident response. This automation accelerates response times by enabling predefined playbooks that initiate actions based on threat intelligence, such as isolating endpoints, updating firewall rules, or enriching incident tickets with CTI context. This integration improves the effectiveness of threat intelligence by embedding it into day-to-day security processes, enhancing situational awareness and ensuring that intelligence is consistently applied across detection, investigation, and response activities.

Splunk's flexible architecture also allows organizations to ingest and correlate CTI from multiple sources without compatibility issues, making it a future-proof solution that grows with an evolving threat landscape. By integrating CTI data feeds and supporting real-time threat correlation with known TTPs, Splunk provides valuable, actionable insights that strengthen defense postures, improve threat visibility, and empower organizations to respond proactively to emerging threats. Through these capabilities, Splunk enables organizations to use threat intelligence strategically, ensuring a more robust and responsive security operation.

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.

Splunk aggregates threat data from open-source feeds, paid subscriptions, and proprietary intelligence. With Splunk and Threat Intelligence Management (TIM), organizations centralize and correlate data for a comprehensive threat view. The platform supports STIX and TAXII standards for seamless integration and analysis. By consolidating threat feeds, Splunk enhances incident detection, response, and prioritization, enabling proactive action against emerging threats.

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.

Splunk's Threat Intelligence Platform consolidates and enriches threat data from open-source, paid, and proprietary sources. Integrated with Splunk, it normalizes data for easier analysis and sharing. Using STIX and TAXII standards, it enables secure distribution of actionable intelligence. The TIP enriches data with context and threat actor profiling, helping teams prioritize responses and integrate with CTI solutions to enhance threat detection and incident response.

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.

Splunk ES and Threat Intelligence Management provide real-time alerts on emerging threats like vulnerabilities, malware, and attack techniques. Alerts include contextual information such as IoCs, threat actor motivations, and mitigations. By integrating with external threat feeds and using advanced analytics, Splunk delivers actionable alerts, helping teams respond quickly, mitigate risks, reduce alert fatigue, and improve response efficiency.

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.

Splunk allows users to define and integrate custom threat intelligence feeds, data sources, and detection rules. It supports custom searches, queries, and machine learning models to tailor insights and alerts to organizational needs. This flexibility enables teams to create personalized, context-aware intelligence, enhancing security operations with targeted threat detection, investigation, and response capabilities specific to their environment.

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.

Splunk integrates with customer-defined feeds, enabling the ingestion of custom threat intelligence, log data, or third-party feeds. It allows users to normalize and correlate this data with other sources, enhancing detection and response. By supporting various formats and protocols, Splunk provides flexible feed integration, ensuring that organizations can tailor their monitoring and security efforts to specific needs, improving visibility and threat detection.

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.

Splunk integrates with SIEM, SOAR, and SOC tools to enhance security operations by collecting and correlating data from various systems for real-time threat detection and response. Its open architecture supports third-party integrations, automating workflows, orchestrating responses, and improving incident management. This creates a unified, efficient security ecosystem, enhancing visibility, incident resolution, and operational efficiency across the security stack.

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.

Splunk offers flexible feed control, integrating premium threat intelligence and custom data. With Splunk ES and TIM, organizations merge high-quality feeds with internal data for enriched context, while adding proprietary IoCs and real-time intelligence. Integration with Splunk SOAR automates responses, improving efficiency and consistency. This comprehensive feed control delivers relevant, actionable insights for effective threat detection and proactive response.

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.

Splunk enables dynamic threat detection through real-time data analysis, leveraging machine learning and advanced analytics to identify anomalies and emerging threats. It continuously monitors and adapts to changing environments, analyzing datasets for suspicious patterns. Splunk's dynamic detection capabilities trigger automated alerts and responses, helping security teams quickly identify, investigate, and mitigate evolving threats across complex infrastructures.

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.

Splunk provides threat context by correlating data from diverse sources, enriching alerts with relevant information like threat intelligence, asset details, and historical data. This context helps security teams understand the scope, severity, and impact of potential threats. By visualizing relationships between incidents and providing actionable insights, Splunk enables informed decision-making, improving incident investigation, response, and overall security posture

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.

Splunk analyzes vast security data in real-time, using machine learning and advanced analytics to detect patterns, identify anomalies, and provide threat visibility. It enriches insights with contextual information to assess severity and impact. Customizable dashboards and automated reports give security teams actionable, data-driven intelligence for faster threat detection 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.

Any Applicable SLA Goes Here

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L14 – Service Category 14: Cybersecurity Threat Intelligence (CTI)

Respondent Name: Hayes e-Government Resources

Solution Name: Zscaler - Zero Trust Exchange

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.

The Zscaler Platform with its ThreatLabz threat intelligence and security research team analyzes 500 trillion data points from the world's largest security cloud, and blocks 9 billion threats per day. The team tracks the most advanced nation-state and cybercrime threat actors and their TTPs to discern emerging attacks and trends.

ThreatLabz researchers have discovered dozens of zero-day vulnerabilities in popular applications and worked with the vendors to address the underlying issues. ThreatLabz has also developed a proprietary malware automation platform, integrated with the Zscaler cloud, that can identify and extract threat intelligence indicators to protect our customers like Florida DMS at scale.

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.

Zscaler's ThreatLabz Research team uses 40+ threat-intelligence feeds to conduct security research, including new and emerging threat analysis. An API can be used to manage custom URL/IP/Domain block lists. Additionally, the Zscaler ThreatLabZ Research team can review any Indicator of Compromise (IOC) and add to global block lists, and in some cases, can also implement an automated custom feed source protocol to ingest customer sourced IOCs.

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.

Zscaler automates threat intelligence collection from over 40 sources, including malware emulation, configuration extraction, open communities, subscriptions, partner and customer sources, and internal signatures. This feeds into Zscaler's security platform, pushing indicators in near real-time. Zscaler's team hunts zero-day vulnerabilities to protect customers and notify vendors, with options for managed threat hunting, threat briefings, and custom threat profiles.

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.

Zscaler Threat Hunting notifies customers of relevant and active threats and incidents. Notifications include overview, technical detail, users details, attack vectors and IoCs. Customers also receive threat briefings tailored to activity and trends. Additionally, Zscaler's Sandbox provides real time threat alerts and blocks malicious files. When a user attempts to download a malicious file, a notification explains the block and logs transactions in real time.

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.

Our platform uses 40+ threat-intelligence feeds to conduct security research, including new and emerging threat analysis. An API can be used to manage custom URL/IP/Domain block lists. Additionally, the Zscaler ThreatLabZ Research team can review any Indicator of Compromise (IOC) and add to global block lists, and in some cases, can also implement an automated custom feed source protocol to ingest customer sourced IOCs.

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.

Zscaler allows customers to integrate private intel feeds using manual or API based CRUD (Create, Read, Update, Delete) workflows to import threat intel into its platform. Customers can submit IOCs (URLs, Domains, IPs, Malicious files/metadata, Yara, Snort) to ThreatLabz, Zscaler's global research team. Zscaler also provides access to MISP platforms for collaboration and information sharing. Zscaler is an active member of CERTs and forums like ACSC, already incorporated into our platform.

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.

Our platform integrates with 100+ partners across the technology landscape categories: Cloud, Identity, Endpoint, Data, Operations, and Network. One of the largest differentiators of our platform is that we integrate with a variety of key zero trust ecosystem technologies including: identity providers, endpoint security services, security information and event management (SIEM) services and public cloud providers. These integrations allow many automations.

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.

Zscaler supports integrating premium feeds and manual intelligence through manual or API based CRUD (Create, Read, Update, Delete) workflows to import threat intel into its platform. Customers can submit IOCs (URLs, Domains, IPs, Malicious files/metadata, Yara, Snort) to ThreatLabz, Zscaler's global research team. Zscaler also provides access to MISP platforms for collaboration and information sharing.

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.

Zscaler Deception's ThreatParse generates a numeric risk score based on dynamic analysis of attacker behavior and indicates severity granularly based on each activity detected. This intel can then be shared with other ecosystem tools like CrowdStrike and Okta for automated actions.

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.

Zscaler’s UVM, part of the Zscaler platform, curates and correlates data from hundreds of sources, in any format and scale. The UVM module aggregates risk factors, mitigating controls, and business context, enabling organizations to understand their risk in a comprehensive and holistic manner for the first time.

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.

Zscaler Unified Vulnerability Management (UVM), part of the Zscaler platform includes many publicly available threat intelligence sources and UVM Insights. UVM Insights is a proprietary blend of threat intelligence sources with ML models that take environmental factors into consideration. Scoring is adjusted and presented based on specific risk factors and controls, providing a prioritized list tailored to the organization's unique environment and risk profile.

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.

Zscaler commits to SLAs with defined service credits and clear performance metrics, ensuring accountability in availability, latency, and security. Specific SLAs include:

- Global Availability: >= 99.999%
- Global Latency: <= 100ms

Zscaler’s SLAs cover latency without exclusions for DLP or malware scanning. Violations are subject to penalties as detailed in each product’s SLA sheet, available at: http://www.zscaler.com/legal/sla-support. For transparency, we provide reporting on proxy latency and offer a real-time public status page for cloud availability at https://trust.zscaler.com. Full Details listed at: https://www.zscaler.com/legal/sla-support

Zscaler’s services are governed by our End User Subscription Agreement, available at https://www.zscaler.com/legal/end-user-subscription-agreement. While we operate as a multi-tenant cloud provider with standard terms, Zscaler is open to negotiating mutually agreeable terms and conditions upon selection as a vendor.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L15 – Service Category 15: Data Security

Respondent Name: Hayes e-Government Resources

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L15 – Service Category 15: Data Security

Respondent Name: Hayes e-Government Resources

Solution Name: Zscaler - Data Protection

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.

Zscaler has a centralized classification engine that is applied uniformly across all channels or contexts where data could be at risk. Zscaler's data security solution, integrated into the Zscaler Platform, protects sensitive information from unauthorized access, loss, and exfiltration across data in use, in motion, and at rest.

With our AI training data, models, input and output data are classified during design and/or automatically via AI guardrails. All AI projects are subject to privacy, compliance and security reviews which validate the data classification. The AI data is protected for confidentiality, integrity and availability based on its classification and system criticality, including in storage.

Powered by AI-driven data visibility, Zscaler's unified platform gives full insight into sensitive data locations and exposure risks, allowing for real-time monitoring and data protection across web, email, private apps, and BYOD endpoints. Cloud-delivered inline DLP, coupled with browser isolation, enforces policies for data in motion, preventing unauthorized access or sharing across channels.

Zscaler's Data Protection solution extends security to data at rest in cloud environments and on endpoints, ensuring that the State's cloud platforms maintain strong security postures. Advanced controls, such as EDM, Indexed IDM, and OCR, enhance data policy enforcement, detecting sensitive data with precision to prevent accidental or malicious exposure.

Seamlessly integrating with existing security frameworks, Zscaler supports compliance with standards like HIPAA, and CCPA, ensuring the State meets regulatory obligations. Centralized policy management allows for consistent data security across the network, with real-time insights into data usage and potential security incidents, minimizing risks and strengthening data security across all environments.

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.

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.

Zscaler’s central classification engine automatically identifies and classifies sensitive data across databases, file shares, cloud storage, endpoints, web, and more. Using predefined dictionaries that leverage AI and Natural language processing, custom dictionaries, boolean logic, IDM, and EDM, Zscaler tags data based on policies and applies real-time protection. Zscaler’s AI engine further enhances detection, identifying sensitive data such as PII.

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.

Zscaler DLP prevents unauthorized data sharing across channels (email, USB, etc.) with a unified policy engine using user context (e.g., username, location) for real-time control. Policies can monitor, warn, or block outbound content, stopping unauthorized data movement. DLP ensures secure protection by operating independently, without relying on external engines, and supports real-time configurations to prevent data loss effectively.

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.

Zscaler’s Data Protection monitors and blocks unauthorized sharing of sensitive data across channels including web, email, sanctioned cloud services, printing, USB, and more. DLP policies allow rules based on user context (e.g., username, department, location), content types, and more, to control data flow in real time. Configurations can be set to monitor, warn/educate, encrypt, or block outbound content, preventing unauthorized copying or movement of sensitive data.

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.

Zscaler's UEBA capabilities use ML to detect anomalies like bulk data uploads/downloads, encrypted uploads, impossible travel logins, inappropriate sharing via SaaS or email domains, and more, producing per-user risk ratings which can also be leveraged in policy.

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.

Zscaler provides the ability to automatically protect against data risks via policy actions based on contextual risk per channel including blocking data transfer, forcing additional authentication, isolating browser sessions, changing shares in SaaS applications, encrypting, alerting, and more. Additionally, Zscaler Workflow Automation provides the ability to prompt or alert users across multiple communications methods, require approvals from managers or administrators.

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.

Zscaler provides audit trails that capture all data-related activities, detailing who accessed sensitive data, actions taken, and timestamps. Our solution offers detailed analytics and reporting for compliance audits, security assessments, and incident investigations, with a differential viewer for in-depth analysis.

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.

Zscaler Data Protection supports compliance with regulatory standards like GDPR, CCPA, and HIPAA through extensive DLP dictionaries and engines. Our solution includes predefined DLP engines and dictionaries and enables custom configurations, allowing organizations to map security controls to specific compliance frameworks. By providing detailed reporting on data access and protection measures, Zscaler helps track compliance status, manage gaps, and meet regulatory requirements.

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.

Data Cataloging and management is inherent to Zscaler's classification engine, and policy enforcement. Zscaler offers integration with data catalog vendors and technology alliance partners (such as Rubrik) for additional functionality.

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.

Zscaler offers integration with data catalog vendors and technology alliance partners (such as Rubrik) for additional functionality.

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.

Zscaler offers integration with data catalog vendors and technology alliance partners (such as Rubrik) for additional functionality.

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.

Zscaler commits to SLAs with defined service credits and clear performance metrics, ensuring accountability in availability, latency, and security. Specific SLAs include:

- Global Availability: >= 99.999%
- Global Latency: <= 100ms

Zscaler's SLAs cover latency without exclusions for DLP or malware scanning. Violations are subject to penalties as detailed in each product's SLA sheet, available at: http://www.zscaler.com/legal/sla-support. For transparency, we provide reporting on proxy latency and offer a real-time public status page for cloud availability at https://trust.zscaler.com. Full Details listed at: https://www.zscaler.com/legal/sla-support

Zscaler's services are governed by our End User Subscription Agreement, available at https://www.zscaler.com/legal/end-user-subscription-agreement. While we operate as a multi-tenant cloud provider with standard terms, Zscaler is open to negotiating mutually agreeable terms and conditions upon selection as a vendor.

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L16 – Service Category 16: Enterprise Security Log Management, Analytics, and Response

Respondent Name: Hayes e-Government Resources

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.

Any applicable Addtional Terms and Conditons Goes Here

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L16 – Service Category 16: Enterprise Security Log Management, Analytics, and Response

Respondent Name: Hayes e-Government Resources

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 Cloud leverages a cloud native microservices architecture.

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.

Any Applicable SLA Goes Here

Any applicable Addtional Terms and Conditons Goes Here