Exhibit D, F, G

Digital Security Solutions

RFP No. 24-43230000-RFP

Revised Attachment L12 – Service Category 12: IT Service Management (ITSM)

Respondent Name: Timothy Masshardt

Solution Name: IRIS Tech, Inc.

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: ITSM Solutions are designed to streamline the delivery and management of IT services by providing a structured approach to incident management, problem resolution, change control, and service request fulfillment. The Solution should support automation, self-service capabilities, and detailed reporting on service levels.

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

IRIS Tech Inc can leverage an ITSM solution that aligns with industry standards such as ITIL (Information Technology Infrastructure Library) to streamline incident management, problem resolution, change control, and service request fulfillment.

Implement a robust incident management module to automate incident detection, assignment, and escalation, ensuring timely resolution and minimizing downtime.

Utilize a problem management module to identify and resolve root causes of incidents, reducing recurrence and improving overall service quality.

Establish a change management module to ensure that all changes to the IT infrastructure are properly assessed, approved, and implemented, minimizing risks and disruptions.

Provide a self-service portal for users to submit service requests, report incidents, and track progress, improving user experience and reducing manual effort.

Configure detailed reporting and analytics to measure service levels, identify areas for improvement, and optimize IT service delivery.

By implementing an ITSM solution with these features, IRIS Tech Inc can improve the efficiency and effectiveness of its IT service delivery, enhance user satisfaction, and reduce costs.

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 Incident Management Workflows – Solution should detect, categorize, and prioritize IT incidents based on predefined rules. The system should support automatic escalation and notification of incidents to the appropriate teams.

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

IRIS Tech, INC can implement an Automated Incident Management Workflow by utilizing a ticketing system that integrates with their existing infrastructure. This system can be configured to detect, categorize, and prioritize IT incidents based on predefined rules, such as incident type, severity, and impact. The system can also be set up to automatically escalate and notify incidents to the appropriate teams, including the Incident Response Team (IRT), ensuring timely response and resolution.

Prompt 3: Self-Service Portal – Solution should enable end-users to submit service requests, track the status of requests, and access knowledge base articles for self-help. The portal should integrate with automated fulfillment workflows, reducing the need for manual intervention.

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

IRIS Tech, Inc. Can develop a Self-Service Portal that enables end-users to submit service requests, track the status of requests, and access knowledge base articles for self-help. The portal will integrate with automated fulfillment workflows, reducing the need for manual intervention.

Prompt 4: Change Management Tools – Solution should include request and approval workflows, risk assessment for changes, and automated enforcement of change windows and rollback plans.

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

Our solution includes request and approval workflows, risk assessment for changes, and automated enforcement of change windows and rollback plans to ensure seamless and secure change management.

Prompt 5: Configuration Management Database (CMDB) – Solution should track all configuration items (CIs) within the IT infrastructure, including hardware, software, networks, and cloud assets. The CMDB should map dependencies between CIs and provide insights into potential impact during incident resolution or change requests.

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

We utilize a formal change management process to document and track all changes to configuration settings, hardware, software, or network infrastructure. This process includes evaluating changes for potential security impacts, such as compliance with CJIS Security Policy and NIST 800-171 controls. Our change management procedures ensure that change requests are approved by the appropriate authorities before implementation.

Prompt 6: Service Level Management – Solution should define, monitor, and report on Service Level Agreements (SLAs). The system should automatically calculate performance metrics such as response time, resolution time, and service availability, and provide real-time dashboards.

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

Solution enables organizations to define, monitor, and report on SLA 's, ensuring transparency and accountability. Key features include:

Automatic calculation of performance metrics, such as response time, resolution time, and service availability.

Real-time dashboards providing instant visibility into SLA performance.

Customizable SLA definitions and thresholds to meet specific organizational needs.

Alerts and notifications for SLA breaches, enabling prompt action and minimzes downtime.

Prompt 7: Pre-Buit Integrations – Solution should include monitoring tools, security platforms, and asset management systems to provide full visibility into the health and performance of IT services.

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

At IRIS Tech, Inc., we understand the importance of seamless integrations to provide comprehensive visibility into IT services. Our solution includes pre-built integrations with popular monitoring tools, security platforms, and asset management systems. This enables our users to streamline their workflows, enhance security, and improve overall IT service management.

Prompt 8: Integration of CTI Data Feeds – provide insights into security incidents or vulnerabilities that could affect IT service delivery, allowing ITSM platforms to correlate service disruptions with known global security threats.

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

Our vulnerability assessment and management solution integrates with CTI data feeds to provide real-time threat intelligence, enhancing vulnerability prioritization by identifying active exploitation campaigns, emerging threats, and vulnerabilities targeted by threat actors.

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. 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.

This Service Level Agreement (SLA) is entered into by and between [Client Name] ("Customer") and IRIS Tech, Inc. ("Service Provider"). This SLA outlines the terms and conditions governing the provision of services, availability, support, and performance of the IRIS platform, a cloud-based Software-as-a-Service (SaaS) solution.

1. Definitions

1.1 IRIS Platform: The Software-as-a-Service (SaaS) platform provided by the Service Provider to the Customer, offering [describe core services of IRIS, e.g., data management, analytics, etc.].
1.2 Service Availability: The percentage of time the IRIS platform is accessible and functioning, excluding scheduled maintenance or Force Majeure events.

1.3 Support Hours: The hours during which the Service Provider offers support services, specified in this agreement.

1.4 Response Time: The time taken for the Service Provider to acknowledge and respond to an issue reported by the Customer.

1.5 Resolution Time: The time taken to resolve a reported issue based on the severity level, as outlined in the SLA.

2. Service Availability

2.1 Uptime Guarantee: The Service Provider guarantees that the IRIS platform will be available 99.9% of the time per calendar month, excluding:

• Scheduled maintenance (as defined in section 5.1).

• Force Majeure events (as defined in section 8).

2.2 Downtime: Any period in which the IRIS platform is inaccessible to the Customer due to technical failures or other issues within the Service Provider’s control.

2.3 Performance Metrics: The Service Provider will monitor platform performance and aim to meet the following targets:

• System Latency: Response times will be under 2 seconds for 95% of all requests.

• Data Processing Time: Critical transactions or processes will be completed in less than 10 seconds. 5659 Strand Court, STE 106, Naples, FL 34110 PH: 239-228-0939 Email: contact@irisintelgroup.com Page 2

3. Support and Incident Management

3.1 Support Hours: Support will be available during the following hours:

- Business Hours: Monday to Friday, 9:00 AM to 6:00 PM EST.

- Emergency Support: 24/7 via emergency support channels (e.g., phone, email).

3.2 Support Channels: The Customer can access support through the following means:

- Email: support@irisintelgroup.com

- Phone: 239-228-0939

3.3 Incident Severity Levels:

- Severity 1 (Critical): Major functionality is down or severely degraded; impacting all users.

- Response Time: Within 1 hour

- Resolution Time: Within 4 hours

- Severity 2 (High): Partial system functionality is impacted, but workarounds are available.

- Response Time: Within 4 hours

- Resolution Time: Within 1 business day

- Severity 3 (Medium): Minor issues that do not impact critical functionality.

- Response Time: Within 1 business day

- Resolution Time: Within 3 business days •

Severity 4 (Low): General inquiries or feature requests.

- Response Time: Within 2 business days

- Resolution Time: Within 5 business days

4. Service Maintenance

4.1 Scheduled Maintenance: The Service Provider will perform regular maintenance to improve and update the IRIS platform. Scheduled maintenance will typically occur during off-peak hours and will be announced at least 72 hours in advance. Notification: The Service Provider will notify the Customer of scheduled maintenance via email and the Customer's dashboard. Duration: The Service Provider will aim to keep scheduled maintenance to a maximum of 4 hours per month. 5659 Strand Court, STE 106, Naples, FL 34110 PH: 239-228-0939 Email: contact@irisintelgroup.com Page 3

4.2 Unscheduled Maintenance: In the event of an emergency, unscheduled maintenance may be required. The Service Provider will notify the Customer as soon as possible.

5. Data Security and Privacy

5.1 Data Protection: The Service Provider will implement reasonable technical and organizational measures to safeguard the security and confidentiality of the Customer's data, in compliance with applicable data protection laws (e.g., GDPR, CCPA).

5.2 Backup and Recovery: The Service Provider will back up Customer data at least once daily. Data recovery is available for up to 7 days of data loss or corruption.

5.3 Data Ownership: Customer retains full ownership of its data. The Service Provider will not access or use Customer data for any purposes other than to provide the service outlined in this SLA.

6. Service Credits

6.1 Eligibility for Service Credits: If the Service Provider fails to meet the uptime guarantee of 99.9%, the Customer may be entitled to service credits. Calculation: Service credits will be calculated as a percentage of the monthly fee paid by the Customer, based on the amount of downtime experienced. Credit Application: The Customer must request service credits within 30 days of the downtime incident.

6.2 Service Credit Schedule:

- 99.0% to 99.9% uptime: 5% credit
- 95.0% to 99.0% uptime: 10% credit
- Below 95.0% uptime: 20% credit

7. Limitations of Liability

7.1 Exclusion of Liability: The Service Provider is not liable for any losses or damages resulting from the following:

- Customers’ failure to comply with the terms of use of the platform.
- Any Force Majeure events (as defined in section 8).
- Delays due to third-party services (e.g., cloud hosting providers). 5659 Strand Court, STE 106, Naples, FL 34110 PH: 239-228-0939 Email: contact@irisintelgroup.com Page 4

7.2 Maximum Liability: The maximum liability of the Service Provider under this SLA is limited to the total fees paid by the Customer for the services in the previous 12- month period.

8. Force Majeure

8.1 Definition: A Force Majeure event refers to any event beyond the reasonable control of the Service Provider, including but not limited to:

- Natural disasters (e.g., earthquakes, floods)
- War, terrorism, or civil unrest
- Strikes or labor disputes
- Failures of third-party service providers

8.2 Notification: The Service Provider will notify the Customer promptly of any Force Majeure event that may impact service delivery.

9. Term and Termination

9.1 Term: This SLA is effective from the start date of the subscription to the IRIS platform and will remain in effect for the duration of the Customer's subscription term, unless terminated earlier as per the terms in the Customer Agreement.

9.2 Termination: Either party may terminate this SLA in the event of:

• Material breach by the other party, if the breach is not cured within 30 days of notification.

• Insolvency or bankruptcy of either party. 10. Governing Law and Dispute Resolution

10.1 Governing Law: This SLA will be governed by and construed in accordance with the laws of the State of Florida.

10.2 Dispute Resolution: Any disputes arising under this SLA will be resolved through mediation in the State of Florida, before escalating to formal legal proceedings.

11. Amendments

11.1 The Service Provider may amend the terms of this SLA by providing 30 days' notice to the Customer. Continued use of the IRIS platform constitutes acceptance of the revised terms.

12. Acknowledgement By signing this SLA, both parties acknowledge and agree to the terms outlined herein.