NeoSystems CMMC Products and Services

A. CMMC Company Compliance Services

NeoSystems offers the following services to support Client's CMMC compliance program: Security Program Management Service, IT Program Management Service, Microsoft 365 Management Service, and Log Management Service (collectively the "CMMC Company Compliance Services"), as more fully described below.

1. Security Program Management

Subject to the Security Program Management Service Exclusions set forth in Section A.1.e., the Security Program Management Service includes initial setup and ongoing operation of a Client's cybersecurity program aligned with the Compliance Requirements, ("Security Program Management Service"), as follows:

a. Initial Setup Tasks

- **i.** Assess the current state of security controls in place for Client's existing In-Scope IT systems.
- **ii.** Create NIST SP 800-171 and CMMC security control list showing the responsibilities, current state, and proposed solution for each applicable control.
- **iii.** Perform a NIST SP 800-171 Basic Assessment and provide summary level score to Client.
- **iv.** Develop a security program roadmap showing recommended security-related projects and initiatives mapped to compliance gaps ("Security Program Roadmap").
- **v.** Create the initial security program documentation deliverables.

b. Initial Setup Document Deliverables

- **i.** Security Control List
- **ii.** Security Program Roadmap
- **iii.** Plan of Actions and Milestones
- **iv.** Information Security Policy
- **v.** Security Awareness Training
- **vi.** Security Role-Based Training
- **vii.** Continuous Monitoring Plan
- **viii.** Incident Response Plan

c. Ongoing Services

- **i.** Assign a fractional Information Security Officer (ISO) to provide information security support to Client.
- **ii.** Perform needed periodic activities to maintain security compliance including risk assessment (annually), security controls review to validate the security posture of the operational environment (annually), review and update security program documentation (annually and as needed), and audit support based on CMMC schedule.
- **iii.** Conduct monthly Security Review meetings with Client representatives to review continuous monitoring activities, performance metrics, past and planned changes to systems and security controls, vulnerability scan results, remediation priorities, and summary of alerts and events.
- **iv.** Provide on-demand access to information security expertise for questions and evaluation of new/changed systems (up to 24 hours per year – see Security Program Management Service Exclusions below).

d. Recurring document deliverables:

- **i.** Security Activity Report (monthly)
- **ii.** Risk Assessment Report (annually)
- **iii.** Security Controls Review (annually)

iv. System Security Plan (annually or as reasonably needed)

v. Updates to security program documentation identified in Initial Setup Document Deliverables (annually or as needed)

e. Exclusions

The following services are excluded from the Security Program Management Service ("Security Program Management Service Exclusions"):

i. Security remediation projects are not included. The Security Roadmap may identify remediation projects to address gaps in cybersecurity compliance that are outside the scope of this SOW. Management or execution of these projects is not included in this SOW. NeoSystems may provide remediation project support and additional managed services for an additional fee on a time and materials basis as set forth in the T&M Labor Rates Table below.

ii. Technical testing is not included. The Security Program Management Service does not include any technical or penetration testing activities. Results of vulnerability scans, if available, will be used as input to the initial assessment. Existing security controls will be assessed based on manual review of system configurations, review of existing documentation, and interviews with Client's staff and support contractors. Ad hoc Support is not included, except as provided herein. The Security Program Management Service includes up to 24 hours per year of on-demand access to security expertise for reasonable requests for security advice throughout the year. NeoSystems expects that the typical request will take less than one (1) hour to complete. Requests exceeding 24 hours cumulative per year or complex requests requiring over two (2) hours to complete will be subject to additional fees, in which event NeoSystems will obtain approval from Client in advance. Security incident investigation and response are subject to time and materials fees as set forth in the T&M Labor Rates Table below.

2. IT Program Management

Subject to the IT Program Management Service Exclusions set forth in Section A.2.e., The IT Program Management Service ("IT Program Management Service") includes initial setup and ongoing management of company-level IT operations aligned with applicable federal compliance requirements.

a. Initial Setup Tasks

i. Perform an assessment and discovery of the existing IT infrastructure equipment, software and services, through series of research, interviews and other discovery methods.

ii. Document assessment findings within the Client's IT Playbook.

iii. Review the findings, omissions, and gaps with the Client during the assessment review meeting.

iv. Discuss process and review templates for onboarding and offboarding of employees.

v. Outline next steps for establishing support and protocols.

vi. Set up user accounts for NeoSystems for administration (if necessary).

b. Initial Setup Document Deliverables

i. IT Playbook document

ii. Network diagram

iii. User Administration document

iv. Workstation Administration document

c. Ongoing Services

i. Update IT Playbook, network diagram, user administration document, and workstation administration document (annually and as needed).

ii. Provide License Management.
iii. Provide Public DNS Management.
iv. Provide External Service Management.
v. Provide IT Budgetary Information

d. **Recurring Document Deliverables**
i. IT Playbook updates (annually or as needed)
ii. Network diagram updates (annually or as needed)
iii. User administration updates (annually or as needed)
iv. Workstation administration updates (annually or as needed)

e. **Exclusions**

The following services are excluded from the IT Program Management Service ("IT Program Management Service Exclusions”):

i. Workstation and server support is not included.
ii. Licenses and associated costs are not included.
iii. IT Program Management support for additional IT Projects that are outside the scope of this SOW are not included. NeoSystems may provide IT project support for IT projects that are outside the scope of this SOW for an additional fee. An additional SOW may be required depending upon the scope of the additional work effort.

f. **Client Responsibilities**
i. Client shall cooperate fully with all requests from NeoSystems to provide information and access to subject matter experts.
ii. Client shall provide administrative access to systems that NeoSystems supports or provides assistance in supporting, e.g., domain registrar, Wi-Fi, firewall, network switches, Windows network, etc.

3. **Microsoft 365 Management**

Subject to the Microsoft 365 Service Exclusions set forth in Section A.3.e., the Microsoft 365 Management Service (“Microsoft 365 Management Service”) includes initial setup and ongoing management of one (1) Microsoft 365 Government Community Cloud ("GCC") or GCC High tenant, as set forth in the In-scope Items Table above, with a security configuration aligned with applicable federal compliance requirements.

a. **Initial Setup Tasks**
i. Establish new Microsoft 365 tenant for Client use.
ii. Set up the user accounts with multifactor authentication.
iii. Establish Microsoft license management with NeoSystems.
iv. Apply secure configuration to the new Microsoft 365.
v. Configure Client’s Microsoft 365 tenant to send security audit logs to NeoSystems log collector (see Log Management Service below).
vi. Migrate data from Client’s existing systems as defined in In-Scope Items Table above to new Microsoft 365 tenant.

b. **Initial Setup Document Deliverables**
i. Microsoft 365 Baseline Status Report
ii. Microsoft 365 License Report

c. **Ongoing Services**
i. Maintain secure configuration for Microsoft 365 tenant
ii. Manage User Accounts and Microsoft 365 licenses.
iii. Manage other Microsoft cloud-based applications to which the Client is subscribed.

- **iv.** Manage security alerts from Microsoft 365.
- **v.** Participate in change management activities for the Microsoft 365 environment including assets, accounts, and software.
- **vi.** Respond to security alerts.

d. Recurring Document Deliverables

- **i.** Microsoft 365 Baseline Status Report (semi-annually)
- **ii.** Microsoft 365 License Report (monthly)

e. Exclusions

The following services are excluded from the Microsoft 365 Management Service ("Microsoft 365 Management Service Exclusions”):

- **i.** Customization of security groups and permissions is not included; SharePoint and Teams sites will be set up for security using default SharePoint security groups (e.g., owner, contributor, visitor) with standard permissions for document libraries and subfolders within sites. NeoSystems may provide support for customizing security groups and permissions for an additional fee, recognizing that this adds complexity to the CMMC compliance effort.
- **ii.** Migration of data from email or collaboration environments other than Microsoft 365/Exchange/SharePoint/Teams is not included but may be available for an additional fee, subject to the limitations of those environments and available migration tools.
- **iii.** The Microsoft 365 Management Service does not include Microsoft 365 licenses. These licenses will be provided by NeoSystems for the fees set forth in the Managed Services Table and the Annual Services Table below.
- **iv.** Deviations from the baseline security policies established by NeoSystems as set forth above that are requested by Client may affect compliance status and may result in additional fees for security evaluation, implementation, testing, and documentation updates.
- **v.** Customization of the Microsoft 365 environment is not included but may be supported by NeoSystems within the constraints of the applicable federal compliance requirements for an additional fee as set forth in the T&M Labor Rates Table below.
- **vi.** Client administrative access to the Microsoft 365 tenant is not included and may adversely affect compliance status resulting in additional fees for compliance monitoring, change management coordination, and documentation updates.
- **vii.** Backups of Office 365 data are not included.
- **viii.** Management of non-Microsoft 365 licenses is not included.

f. Client Responsibilities

- **i.** Client is solely responsible for meeting Microsoft’s qualification criteria for obtaining GCC or GCC High licenses and shall purchase the same within a reasonable time following the Effective Date.
- **ii.** Client shall identify and provide NeoSystems with administrative access to existing data stores, whether on-premises or cloud hosted.
- **iii.** Client shall communicate via Ticket for all moves, adds, changes (MACs) of employees, licenses, and equipment within the M365 tenant. To submit a Ticket, Client must send an email to support@neosystemscorp.com (the “Ticket”) requesting desired changes or additional services. By submitting a Ticket, Client agrees to bear the pricing and scheduling impacts of such Ticket. Each Ticket is incorporated into this SOW by reference.
- **iv.** Client shall provide NeoSystems two (2) weeks’ notice in advance of a new employee’s start date.

- **v.** Client shall provide clear and concise communications regarding how to handle a departing employee's data. If a license is removed from an account, data may be removed in as little as thirty (30) days.
- **vi.** Client shall review and approve the list of users and data to be migrated and the permissions tables for the target environment.
- **vii.** If data paths on existing data stores exceed the limitations of the migration tools or the target environment, Client shall shorten the paths by re-naming or re-organizing the directory tree hierarchy. NeoSystems may provide support for path clean-up for an additional fee.
- **viii.** Unless otherwise provided herein, Client shall migrate data into new SharePoint sites.
- **ix.** Client shall notify NeoSystems in advance if data to be migrated contains CUI or other controlled information so that NeoSystems can arrange for protection of the data (e.g., schedule migration after hardening of target environment and/or protect data in transit).

4. Log Management (if selected)

Subject to the Log Management Service Exclusions set forth in Section A.4.e., the Log Management Service includes initial setup and ongoing operation of cloud-based centralized log management for security logs from identified log sources within Client's IT environment ("Log Management Service"), as follows:

a. Initial Setup Tasks

- **i.** Perform log collection either with (i) agents on individual source devices or; (ii) one or more log collector appliances within Client's on-premises and/or cloud computing environment(s).
- **ii.** Provide audit log collector software agents and/or virtual software appliances for installation in Client's IT environment (on-premises and/or cloud).
- **iii.** Configure log collector agents and/or virtual appliances to establish secure host-to-host virtual private network communication with NeoSystems' centralized log management platform.
- **iv.** Configure log ingest parsers and filters for identified log sources.
- **v.** Configure alerts for known-bad or suspicious events by log type.
- **vi.** Configure escalation and reporting processes.

b. Initial Setup Document Deliverables

- **i.** Inventory of Log Sources

c. Ongoing Services

- **i.** Maintain log collector appliance(s).
- **ii.** Manage collection and retention of audit logs from covered IT assets.
- **iii.** Review audit logs for suspicious or unauthorized activity.
- **iv.** Analyze and triage events to support event resolution and incident declaration.
- **v.** Monthly Security Review meeting to review activity, alerts, and tuning recommendations.
- **vi.** Initiate investigations, alerts, and escalations as appropriate to respond to suspicious or unauthorized activity.
- **vii.** Retain logs for 90 days in our active system and 365 days in archival format.
- **viii.** NeoSystems will provide, configure, and maintain all necessary application software for Client's Log Collector VMs.

d. Recurring Document Deliverables

i. Log Management Executive Report (monthly)

e. **Exclusions**
The following services are excluded from the Log Management Service ("Log Management Service Exclusions"):

i. Installation of log collector agents is outside the scope of the Log Management Service. Installation may be performed as part of Server Management Service, if selected, or by Client.

ii. Configuration of the log sources to generate the desired audit logs and forward them to the log collector agent/appliance using a mutually agreed upon protocol (e.g., *syslog*) is outside the scope of the Log Management Service. Configuration may be performed by NeoSystems as part of other Services described herein, if selected, or by Client.

iii. Configuration of network devices to enable connectivity between deployed log collector agents/appliances and NeoSystems' cloud-based management platform is outside the scope of the Log Management Service. Configuration may be performed by NeoSystems as part of the Network Management Service, if selected, or by Client.

iv. Changes or break-fix in log source ingest setup due to changes in log sources after initial setup are outside the scope of the Log Management Service and will be provided on a time and materials basis as set forth in the applicable Statement of Work and may be requested by Ticket.

v. Changes to the log sources (such as upgrades or technology refreshes) which necessitate changes to the log collection, parsing, or alert configuration are outside the scope of the Log Management Service may be requested by Ticket and will incur additional charges.

vi. Assistance with and/or the performance of setup or administration of Log Collector VMs (as defined below), are outside the scope of the Log Management Service and may be provided at Client's request on a time and materials basis as set forth in the applicable SOW.

f. **Client Responsibilities.**

i. Client shall identify the log sources to be collected by the Log Management Service and shall notify NeoSystems of any additions or changes to the log sources.

ii. Client shall provide appropriately sized physical or virtual machines for on-premise or cloud-based log collector appliance(s) ("Log Collector VMs").

B. CMMC Workstation and Server Compliance Services

NeoSystems offers the following services to support Client's In-Scope end user workstations and servers for CMMC compliance: Workstation Management Service, Server Management Service, Endpoint Protection Service, and Vulnerability Scanning Service (collectively the "CMMC Workstation and Server Compliance Services"), as more fully described below.

1. Workstation Management

Subject to the Workstation Management Service Exclusions set forth in Section B.1.e, the Workstation Management Service ("Workstation Management Service") includes initial setup and ongoing management of Windows devices, as set forth in the In-scope Items Table above, with a security configuration aligned with applicable federal compliance requirements.

a. **Initial Setup Tasks**

i. Establish tenant for Client in NeoSystems' centralized Remote Monitoring & Management ("RMM") console.

ii. Configure RMM console with organization and group tags for identification of devices.

iii. Establish initial patching schedule and criteria.

iv. Install RMM agents on in-scope Windows devices.

v. Enroll workstations in M365 so they can be managed via Azure AD & InTune policies.

vi. Apply secure configuration to all in-scope workstations. Apply patches to Windows operating systems and major third-party applications found at https://documentation.n-able.com/N-central/userguide/Content/Patch-Management/PatchManagement_3Party_Patch_List.htm, or in response to notices from the software vendor and third-party sources such as federal security alerts to in-scope Windows workstations.

vii. Install software agents for Endpoint Protection Service, Vulnerability Scanning Service, and Log Management Service.

b. Initial Setup Document Deliverables

i. Active Asset inventory

c. Ongoing Services

i. Apply updated secure configuration to in-scope Windows workstations.

ii. Provide patch management which includes updates to Microsoft Windows operating system and major third-party applications, found at https://documentation.n-able.com/N-central/userguide/Content/Patch-Management/PatchManagement_3Party_Patch_List.htm, or in response to notices from the software vendor and third-party sources such as federal security alerts.

iii. Apply commercially available remediations to identified vulnerabilities of workstations listed in the In-scope Items Table.

iv. Conduct daily safety checks such as physical disk health checks, failed login attempts, drive space changes, and critical events from the application, security, and system logs.

v. Conduct 24/7 performance checks throughout the day on Windows machines to ensure that the performance of machines is not compromised.

vi. Provide remote technical support, following Client's submission of a Ticket, using our US-based technicians, including user administration, application support for Microsoft Office, and hardware troubleshooting.

vii. Remediate vulnerabilities that patching does not address.

d. Recurring Document Deliverables

i. Active Asset Inventory Report

ii. Patch Management Report

e. Exclusions

The following services are excluded from the Workstation Management Service ("Workstation Management Service Exclusions"):

i. NeoSystems is not directly responsible for hardware repairs. All hardware repairs must be performed by the manufacturer or the manufacturer's subcontractor according to the equipment's maintenance agreement.

ii. NeoSystems does not provide support for applications that are not under an active subscription or maintenance agreement.

iii. The Workstation Management Service does not include Microsoft Windows license(s) or application software license(s). These licenses may be provided by NeoSystems for additional Fees or provided by Client. All in-scope devices must have licensed software with an active vendor support agreement. End-of-life software is not supported and may adversely affect compliance status.

iv. Support for end-of-life applications and operating systems is not included.

v. Support for software or hardware on workstations that are not under a maintenance agreement is not included.

vi. Support for Client-supplied applications not on the third-party list may be supported by NeoSystems in its sole and absolute discretion

vii. Functional support for applications is not included.

viii. Backups for workstations or Microsoft 365 are not included.

ix. Workstations with other than Microsoft Windows 10/11 Pro or Enterprise are not supported.

x. NeoSystems will not provide patching and remediation for:

(a) Workstations which are not listed in the In-scope Items Table.

(b) Applications which are not listed in the In-scope Items Table.

(c) Vulnerabilities which have not been detected.

(d) Remediations which are not commercially available.

f. Client Responsibilities

i. Client shall identify the devices to be supported by the Workstation Management Service and Server Management Service and shall provide NeoSystems with administrative access to facilitate installation of the RMM agent software and application of the baseline security policies.

ii. Client shall backup all end-user data prior to system re-configuration/re-build by NeoSystems. NeoSystems is not responsible for lost user data.

iii. Client is responsible for identifying CUI and other controlled information on end-user workstations so that NeoSystems can arrange for protection of the data.

iv. Client shall notify NeoSystems of any additions or changes to the workstations. When a workstation is taken out of service for any reason, e.g., reimaging, reassignment, or retirement, charges will continue until Client notifies NeoSystems of the change.

2. Server Management

Subject to the Server Management Service Exclusions set forth in Section B.2.e, the Server Management Service ("Server Management Service") includes initial setup and ongoing management of servers, as set forth in the In-scope Items Table above, with a security configuration aligned with applicable federal compliance requirements.

a. Initial Setup Tasks

i. Establish tenant for Client in NeoSystems' centralized RMM console.

ii. Install RMM agents on in-scope Windows devices.

iii. Configure RMM console with organization and group tags for identification of devices.

iv. Set up baseline security policies and software updates to in-scope Windows Servers in accordance with industry benchmarks aligned with federal compliance requirements.

v. Install and configure software agents for Endpoint Protection Service, Vulnerability Scanning Service, and Log Management Service, if selected.

b. Initial Setup Document Deliverables

i. Active Asset inventory

ii. Patch Management Report

c. Ongoing Services

i. Apply updated baseline security policies to in-scope Windows Servers.

ii. Provide patch management which includes updates to Microsoft Windows operating system and major third-party applications, found at https://documentation.n-able.com/N-central/userguide/Content/Patch-Management/PatchManagement_3Party_Patch_List.htm, or in response to notices from the software vendor and third-party sources such as federal security alerts.

iii. Apply commercially available remediations to identified vulnerabilities of servers listed in the In-scope Items Table.

iv. Conduct daily safety checks such as physical disk health checks, failed login attempts, drive space changes, and critical events from the application, security, and system logs.

v. Conduct 24/7 performance checks throughout the day on Windows machines to ensure that the performance of machines is not compromised.

vi. Provide remote technical support, following Client's submission of a Ticket, using NeoSystems' US-based technicians, including user administration, application support for Microsoft Office, and hardware troubleshooting.

d. Recurring Document Deliverables

i. Active Asset Inventory Report

ii. Patch Management Report

e. Exclusions

The following services are excluded from the Server Management Service ("Server Management Service Exclusions"):

i. NeoSystems is not directly responsible for hardware repairs. All hardware repairs must be performed by the manufacturer or the manufacturer's subcontractor in accordance with the equipment's maintenance agreement.

ii. Support for applications that are not under an active subscription or maintenance agreement is not included.

iii. The Server Management Service does not include Microsoft Windows license(s) or application software license(s). These licenses may be provided by NeoSystems for additional Fees or provided by Client. All in-scope devices must have licensed software with an active vendor support agreement. End-of-life software is not supported and may adversely affect compliance status.

iv. End-of-life operating systems and applications are not included.

v. Support for software or hardware on workstations that are not under a maintenance agreement is not included.

vi. Functional support for applications is not included.

vii. Backups for servers are not included.

viii. NeoSystems will not provide patching and remediation for:

(a) Servers which are not listed in the In-scope Items Table.

(b) Applications which are not listed in the In-scope Items Table.

(c) Vulnerabilities which have not been detected.

(d) Remediations which are not commercially available.

f. Client Responsibilities

i. Client shall provide administrative access to the servers.

ii. Client shall identify the devices to be supported by the Server Management Service and shall provide NeoSystems with administrative access to facilitate installation of the RMM agent software and application of the baseline security policies.

iii. Client shall backup all end-user data prior to system re-configuration/re-build by NeoSystems. NeoSystems is not responsible for lost user data. NeoSystems may support backup of end-user data on a time and materials basis as set forth in the T&M Labor Rates Table below.

iv. Client shall identify CUI and other controlled information on servers so that NeoSystems can arrange for protection of the data.

v. Client shall notify NeoSystems of any additions or changes to the servers. When a server is taken out of service for any reason, e.g., reimaging, reassignment, or retirement, charges will continue until Client notifies NeoSystems of the change.

3. Endpoint Protection

Subject to the Endpoint Protection Service Exclusions set forth in Section B.3.d, the Endpoint Protection Service ("Endpoint Protection Service") includes initial setup and ongoing management of non-signature-based anti-malware protection on Windows devices, as set forth in the In-scope Items Table above, with a security configuration aligned with applicable federal compliance requirements.

a. **Initial Setup Tasks**
   - **i.** Provide and maintain endpoint protection agents for all in-scope endpoint devices.
   - **ii.** Configure endpoint protection to perform automated detection, blocking of threats, and alerting of suspicious events.

b. **Ongoing Services**
   - **i.** Analyze and triage alerts to support event resolution and incident declaration.
   - **ii.** Escalate suspicious events to IT staff.
   - **iii.** Report on threats detected and resolutions.

c. **Recurring Document Deliverables:**
   - **i.** Endpoint Threat Summary (monthly)

d. **Exclusions**

   The following services are excluded from the Endpoint Protection Service ("Endpoint Protection Service Exclusions”):
   - **i.** Installation of endpoint protection agents is outside the scope of the Endpoint Protection Service, and may be performed by NeoSystems as part of Server Management Service, if selected, or performed by Client.
   - **ii.** Configuration of Client’s network to enable connectivity between deployed endpoint protection agents and NeoSystems’ cloud-based management platform is outside the scope of the Endpoint Protection Services. NeoSystems will assist with the configuration of network devices at Client’s request by Ticket for an additional Fee.

e. **Client Responsibilities.**
   - **i.** Client shall identify the endpoints to be covered by this service.
   - **ii.** Client shall install the software agents provided by NeoSystems on each endpoint.
   - **iii.** Client shall configure its network to enable connectivity between deployed endpoint protection agents and NeoSystems’ cloud-based management platform.
   - **iv.** Client shall notify NeoSystems of any additions or changes to the list of covered endpoints. When a covered endpoint is taken out of service, re-imaged, or re-assigned, charges will continue on the endpoint until Client notifies NeoSystems of the change.

4. Vulnerability Scanning

Subject to the Vulnerability Scanning Service Exclusions set forth in Section B.4.d, the Vulnerability Scanning Service (“Vulnerability Scanning Service") includes initial setup and ongoing management of vulnerability scans of in-scope devices, as set forth in the In-scope Items Table above, in alignment with applicable federal compliance requirements.

a. **Initial Setup Tasks**
   - **i.** Provide vulnerability scanner agents and/or virtual appliances for installation in Client’s IT environment (on-premises and/or cloud).
   - **ii.** Configure vulnerability scanner agents and/or virtual appliances to establish secure host-to-host virtual private network communication with NeoSystems’ centralized vulnerability management platform.
   - **iii.** Configure vulnerability scanner agents and/or virtual appliances within Client’s network as needed to perform internal scans of all identified Internet Protocol (IP) addresses.
   - **iv.** Establish recurring monthly scanning and reporting.

b. **Ongoing Services**

i. Conduct monthly vulnerability scans of all external and internal Client IP addresses using a comprehensive, up-to-date list of vulnerabilities. Authenticated scans will be performed at Client's option and provide more detailed results than non-authenticated scans.

ii. Provide summary reporting that includes scan metrics such as systems scanned, vulnerability counts, and vulnerability aging.

iii. Provide detailed scan results as a Comma Separated Values (CSV) file for use by IT staff who will remediate identified vulnerabilities.

iv. Provide no more than two (2) on-demand scans per month to validate remediation or to scan new or changed systems. On-demand scans will be performed within one (1) to three (3) business days of the request depending on resource availability.

v. Provide, configure, and maintain all necessary application software for on premise or cloud-based vulnerability scanners for which Client has provided appropriately sized virtual machines.

c. Recurring Document Deliverables:

i. Vulnerability Scan Summary Report (monthly)

ii. Vulnerability Scan Results (monthly and per scan for on-demand scans)

d. Exclusions

The following services are excluded from the Vulnerability Scanning Service ("Vulnerability Scanning Service Exclusions"):

i. On-demand scans are intended to cover a limited number of systems (e.g., new or changed systems). On-demand scan requests in excess of two (2) per month are outside the scope of the Vulnerability Scanning Service and may be requested by Ticket for an additional Fee.

ii. Setup of credentials for an account with administrative privileges to facilitate authenticated scanning is outside the scope of the Vulnerability Scanning Service and may be performed by NeoSystems as part of Server Management Service, if selected, or be performed by Client.

iii. Configuration of network devices to enable connectivity between deployed scanner agents/appliances and NeoSystems' cloud-based management platform is outside the scope of the Vulnerability Scanning Service and may be performed by NeoSystems as part of the Network Management Service, if selected, or performed by Client.

iv. Identifying the Internet Protocol (IP) addresses and/or ranges to be scanned during vulnerability scans is outside the scope of the Vulnerability Scanning Service. At Client's request by Ticket, NeoSystems will perform network mapping and discovery to determine the IP addresses in use in Client's network for an additional Fee.

v. Provision of appropriately sized Vulnerability Scanner VMs for on premise or cloud-based vulnerability scanners is outside the scope of the Vulnerability Scanning Services. At Client's request by Ticket, NeoSystems will perform setup and administration of these Vulnerability Scanner VMs for an additional Fee.

e. Client Responsibilities

i. Client shall identify the Internet Protocol (IP) addresses and/or ranges to be scanned during vulnerability scans and shall notify NeoSystems of any additions or changes to the IP addresses.

ii. Client shall provide appropriately sized virtual machines for on premise or cloud-based vulnerability scanners ("Vulnerability Scanner VMs").

iii. Client must provide account credentials to NeoSystems.

C. CMMC Network Compliance Services

NeoSystems' Network Compliance Services provide management and support of routers, firewalls, switches, and wireless access points. Firmware updates are performed as a part of routine maintenance. Configuration updates may be requested via Ticket.

1. Network Management

Subject to the Network Management Service Exclusions set forth in Section C.1.d, the Network Management Service ("Network Management Service") includes initial setup and ongoing management of network devices, as set forth in the In-scope Items Table above, with a security configuration aligned with applicable federal compliance requirements.

a. Initial Setup Tasks

- **i.** Review existing network configuration (if applicable) for adherence with compliance requirements.
- **ii.** Configure In-Scope network device(s) for remote management and monitoring.
- **iii.** Apply baseline security policies and software updates to In-Scope network device(s) in accordance with industry benchmarks aligned with CMMC requirements.

b. Ongoing Services

- **i.** Apply firmware updates in response to notices from the software vendor and third-party sources such as federal security alerts.
- **ii.** Monitor Internet availability.
- **iii.** Apply changes to the network configuration as needed to facilitate Client use of the network and maintain security compliance.

c. Recurring Document Deliverables

- **i.** Network Availability Report
- **ii.** Sonicwall Firmware Report (if applicable)

d. Exclusions

- **i.** Management of network devices other than Cisco, Fortinet and SonicWall is not supported by the Network Management Service.
- **ii.** Redesigns of network architecture, e.g. complete VLAN restructuring, HA pair introduction are not included.
- **iii.** Troubleshooting issues with user's home networks is not included.
- **iv.** Hardware upgrades are not included in the Network Management Service. NeoSystems may support hardware upgrades for an additional fee on a time and materials basis as set forth in the T&M Labor Rates Table below.
- **v.** The Network Management Service does not include network hardware or support agreements. If marked as "new" in the In-scope Items Table above, these items will be provided by NeoSystems for the fees set forth in the Third-Party Products Table below. If marked as "exist" in the In-scope Items Table above, these items must be provided by Client and must have an active vendor support agreement.
- **vi.** End-of-life devices are not supported by the Network Management Service and may adversely affect compliance status.
- **vii.** Deviations from baseline security policies established by NeoSystems as set forth above that are requested by Client may affect compliance status and may result in additional fees for security evaluation, implementation, testing, and documentation updates.

D. Additional Support Services

NeoSystems offers the following additional services on a time and materials basis as set forth in in the applicable Statement of Work: Incident Response Service, and Ad Hoc Support Services (collectively the "Additional Support Services"), as more fully described below.

1. Incident Response

The Incident Response Service ("Incident Response Service") includes on-demand support for investigation of suspicious events and response to security incidents in accordance with the established Incident Response Plan and applicable federal compliance requirements. This service applies to all security incidents that meet the criteria for formal incident reporting and/or require investigation to determine the cause or extent of the incident. This service provides compliance with the specific incident handling requirements of CMMC and DFARS 252.204-7012. All Incident Response Services are provided on a time and materials basis as set forth in the applicable Statement of Work.

a. As-needed Services

i. Accept incident reports from Client via Ticket.

ii. Provide case management, response coordination, communications, and required reporting for security incidents.

iii. Perform incident investigation, analysis, and response activities.

b. Recurring Document Deliverables

i. Incident Ticket Report (per incident)

2. Ad Hoc Support

Client may request security and IT support services for Client that are beyond the scope of the CMMC Compliance Services and Incident Response Services on an ad hoc basis by Ticket, which may be accepted by NeoSystems in its sole discretion ("Ad Hoc Support Services"). Any such Ad Hoc Support Services shall be provided on a time and materials basis as set forth in the applicable Statement of Work.