Managed Security Service (MSS)

The EIS Managed Security Service is a comprehensive service that protects an agency's information technology assets—hardware devices, network, software, and information—from malicious attacks. It includes capabilities such as authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management. MSS comprises:

- **Managed Prevention Service (MPS**)
  Monitors computer devices, network traffic, email, and application activity to identify and mitigate suspicious activity.

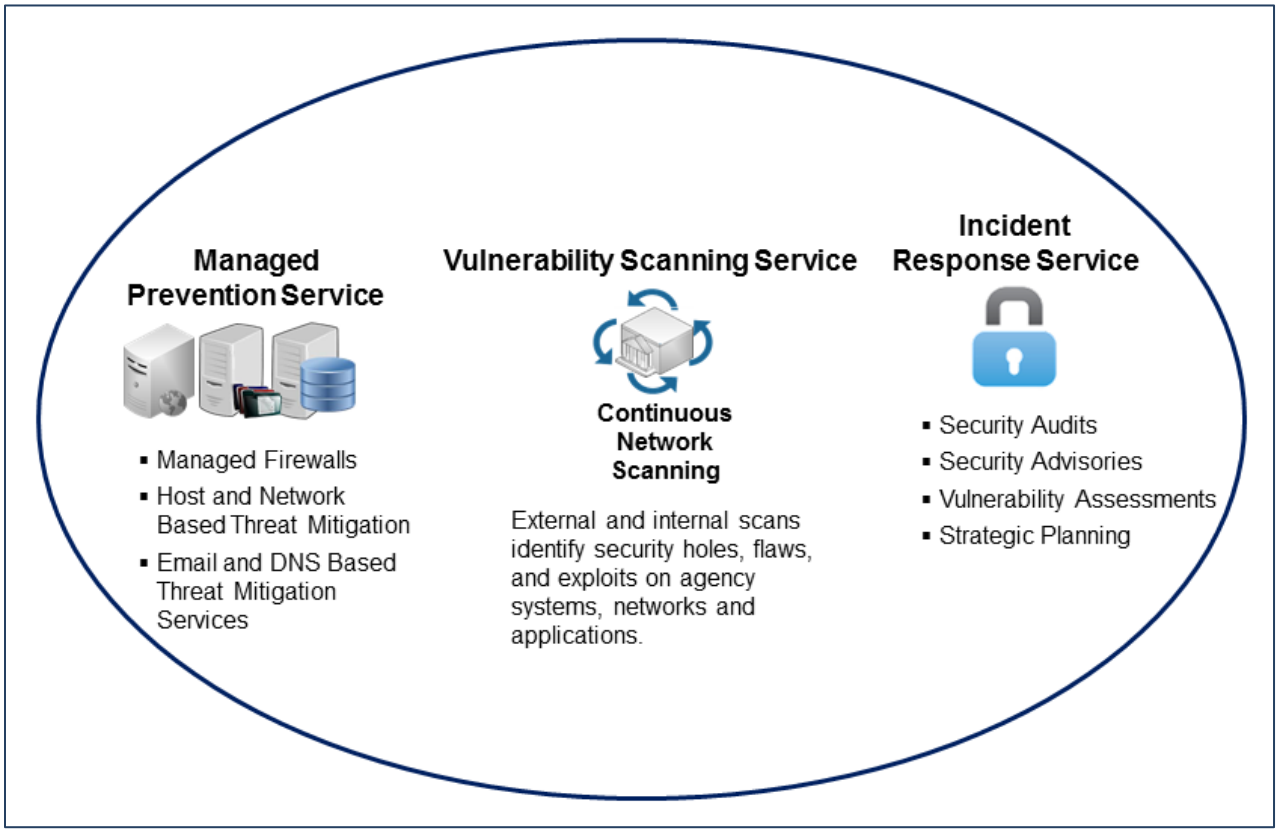
- **Vulnerability Scanning Service (VSS)**
  Performs external scans by remotely probing a network for vulnerabilities, and internal scans to detect flaws originating from the inside.

- **Incident Response Service (INRS)**
  Provides an effective method of combatting and documenting security intrusions, thereby ensuring operational continuity and the capture of forensics data that can assist in apprehending and prosecuting offenders. INRS consists of both proactive and reactive activities.

Category: Managed Services

Definitions: Please see EIS contract Section J.12 Glossary of Terms for clarification of technical terms and acronyms.

Figure 1—The EIS Managed Security Service consists of the three main functions shown below.



1. Why an Agency Might Select this Service

- An agency needs a proven set of security tools and procedures to combat the ever growing threat of cyberattacks from cybercriminals and corrupt organizations. MSS can fill this need for an agency, and free up the organization to focus more on its mission.

- MSS provides a systematic approach to managing an organization's enterprise network security needs. The service continuously monitors network devices and traffic for suspicious activity, regularly scans for vulnerabilities, and enables the agency to quickly respond to cyberattacks.

- In many cases, a contractor devoted to security issues can better meet the ever increasing volume and sophistication of cyberattacks than an agency faced with skill shortages and resource constraints.

NOTE: Agencies considering this service may also want to compare this service with Managed Network Services (MNS) and Managed Trusted Internet Protocol Service (MTIPS).

2. Examples of How MSS Could be Used

- **Provide End-to-End Cybersecurity:** An agency could use MSS to provide end-to-end cybersecurity including round-the-clock monitoring, management of intrusion detection systems and firewalls, patch and upgrade management, security audits, and cyberattack response.

- **Detect and Stop Denial of Service Attacks:** The MSS Incidence Response Service could assist an agency during a Distributed Denial of Service attack (DDoS). (A DDoS takes place when an overwhelming amount of illegitimate traffic is maliciously pushed to the agency's network with the purpose of making the network unavailable for its intended use.) INRS processes can detect such an attack and provide the processes and security tools to counter the DDoS and restore operation of the system.

3. Key Technical Specifications

NOTE: This portion of the service guide has been abridged due to space considerations. For full technical details on MSS, please refer to EIS contract Section C.2.8.5 Managed Security Service.

Table 1—MSS Technical Capabilities

Capability	*Description*
Managed Prevention Service (MPS)	1. Design and implementation services that enable the agency and the contractor to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures. 2. Software and hardware components, including log servers. 3. Hardware or software load balancing capabilities and redundancy. 4. Installation support to include testing of equipment, testing of software, and loading of any agency-relevant data. 5. Maintenance of latest configuration information for restoration purposes, reporting, and forensics analysis. 6. Managed service capabilities, performing hardware/software upgrades and replacements, and content updates. 7. See contract for details. 8. Agency notification of patches and bug fixes as soon as they become available. 9. Testing and deployment of the latest patches and bug fixes as soon as they become available and are approved by the agency. 10. Document configuration and management to ensure that security, access, and information-flow policies are enforced. 11. to 20. See contract for details. 21. Secure web access to logs and service information including the following: a. Active Sessions b. Port and Protocol Activity c. Authentication Statistics d. Connections/Attempts counts and results (accepted/rejected) by port e. Events, rule violations, and attacks detected including name,description, level, impact date, time, vulnerabilities and targeted weakness, and remedies f. Source and Destination IP Addresses, domains (fully-qualified domain name) and URLs; as well as statistics g. Affected endpoints h. Managed Prevention Service Statistics and Utilization i. Outages j. Configuration Modifications k. Change Requests and Event Tickets

Capability	*Description*
Vulnerability Scanning Service (VSS)	Supports the agency in establishing, implementing and maintaining a vulnerability scanning service on a 24x7 basis. Includes: 1. External Vulnerability Scanning which tests Internet-connected nodes in the network, including web environments. 2. Internal Vulnerability Scanning which looks for local/host flaws and internal threats, usually inside the firewall. Periodically probes networks, including operating systems and application software, for potential openings, security holes, and improper configuration. Probes agency systems for vulnerabilities in a wide variety of areas such as: Back Doors, Common Gateway Interface, DNS, etc. (See Section C.2.8.5.1.4.2 Vulnerability Scanning Service for a complete list of areas that VSS can probe.) In addition to the above, the contractor is responsible for the following tasks: 1. Proactively identifies network vulnerabilities and proposes appropriate countermeasures, fixes, patches, and workarounds. 2. Notifies the agency of vulnerabilities discovered via email, fax, or telephone, as directed by the agency. 3. Provides the agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses. 4. Reviews vulnerabilities discovered with the agency, as required. 5. Provides scan scheduling flexibility to the agency in order to minimize any interruptions in normal business activities. 6. Provides the agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed or disrupt agency operations. These scans do not provoke a denial of service condition on the system being probed. 7. Uses other analytical means to ascertain the vulnerability of agency systems if a particular scan is potentially destructive or intrusive. 8. Ensures that the scanning engine is regularly updated with new vulnerabilities information in order to maintain effectiveness of the service. 9. Supports networks of varying size and complexity.

Capability	*Description*
Incident Response Service (INRS)	As part of INRS, the contractor performs the following tasks: 1. Reviews the agency's security infrastructure and develops appropriate strategic plans in collaboration with the agency. These plans detail the incident response process, identify internal resources, assign duties to team members, describe policies, define severity levels, list escalation chains, and specify emergency/recovery procedures. 2. Provides the agency with effective incident response support on a 24x7 basis. 3. Maintains a problem detection system for the diagnosis of alerts and violations. 4. Analyzes suspicious security alerts to determine the significance and scope of an event and immediately notify the agency when the event is deemed high priority. 5. Provides the agency with immediate access to vulnerability and severe alert information, which minimally contains the following: Description, Target, Origin, Potential Incident Impacts, Remedies, Prevention Measures. 6. Coordinates with the agency to handle potential security incidents according to the appropriate response procedures. 7. Provides countermeasures to contain the security incident, limit its spread, and protect internal systems 8. Recommends the fixes necessary to eliminate identified vulnerabilities, and appropriate procedures to guard against future attacks. 9. Provides the agency with secure web access to incident analysis findings and recommendations.

Table 2—MSS Features

Feature	*Description*
Managed Prevention Service (MPS)	Please see EIS contract Section C.2.8.5.2 Features for the details on each of the following Managed Prevention Service features: a) Firewall b) Personal Firewalls c) Network Intrusion Prevention System d) Endpoint Protection e) Secure Web Proxy f) Inbound Web Filtering g) Application-Level Gateway protocols (FTP, SIP, IM, etc.) to be proxied. h) Network Behavior Analysis i) Network Traffic Content Analysis and Sandboxing j) Email Forgery Protection and Filtering k) Email Content Analysis and Sandboxing l) User Authentication Integration m) DNSSEC n) DNS Sinkholing o) Data Loss Prevention p) Demilitarized Zones (DMZs) Support q) Extranet Support r) Firewall-to-Firewall VPNs s) Remote Client VPNs t) EINSTEIN 2 u) Short-Term Storage v) Long-Term Storage w) Agency-specified policy enforcement.
Vulnerability Scanning Service (VSS)	VSS API: The contractor provides the agency with the ability to integrate the service into its own tools and applications, using for example, standard XML and RESTful APIs, as required by the agency. This assists in-house security personnel with tasks such as scanning IP addresses, assessing host vulnerabilities, creating user accounts, and exporting vulnerability data.
Incident Response Service (INRS)	Advanced Analytics: The contractor provides and applies various statistical techniques from the modeling, machine learning, and data mining disciplines to analyze relevant observations for threat discovery, assessment, situational awareness, and prediction. Where applicable, the techniques provided yield confidence intervals establishing the statistical significance of findings. When statistical significance cannot be established using rigorous, state-of-the-art techniques, the findings include this caveat.

4. Pricing Basics for MSS

Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide to gain an understanding of EIS pricing fundamentals.

4.1 Access Arrangements

No access arrangements are needed for MSS.

4.2 Service Related Equipment (SRE)

- SRE must be chosen based on equipment required at each location. NOTE: SRE uses catalog-based pricing.
- Request that contractor provide pricing for any SRE that would be required, in addition to the agency's existing infrastructure, to deliver the service.
- Please visit the EIS Resources Listing and locate the Service Related Equipment Service Guide for more detailed information.

4.3 MSS Price Components

MSS pricing is provided by the contractor in an MSS service catalog. This catalog contains items as specified in EIS contract table *B.2.8.5.2—Managed Security Service Catalog – Product Specification Table*.

The catalog items are divided into three categories for which the contractor can define Non-Recurring Charge (NRC), Monthly Recurring Charge (MRC), and Usage items as shown in *Table 3* below. A contractor, for example, could define "Managed Prevention Service Initiation" as all the tasks needed to set up the Managed Security Service for an agency. This would be a one-time service with an associated NRC.

Table 3—MSS Pricing Components

Component	*MSS Catalog Item*	*Charging Unit*
Managed Prevention Service	NRC, MRC, or Usage	Individual Case Basis (ICB)
Vulnerability Scanning Service	NRC, MRC, or Usage	ICB
Incident Response Service	NRC, MRC, or Usage	ICB

Figure 2 below shows how the pricing components in *Table 3* are combined to produce the total cost for the service.

Figure 2: This figure shows how the various pricing components in Table 3 would be combined to calculate the total MSS charges. NOTE: One or more of these components may not be needed to price a particular service.

The charges for the different components in *Figure 2* are calculated with the help of the pricing tables in EIS contract Section B.2.8.5 Managed Security Service. (Please visit the EIS Resources Listing and locate the Basic EIS Pricing Concepts Guide for a detailed explanation of the catalog pricing tables, and how they are used to price a service.)

NOTE: A contractor may offer a custom variation of the service to meet an agency's unique requirements. Such a customized service would be identified with a Task Order Unique CLIN (TUC), and could include charges in addition to those shown in *Figure 2* above.

4.4 MSS Pricing Examples

No pricing examples are provided for Managed Security Service, as all pricing is catalog-based.

Please see the EIS Basic Pricing Concepts Guide for instructions on using an EIS catalog.

5. References and Other Sources of Information

- For more technical details and information on MSS, please refer to EIS contract Section C.2.8.5; for pricing details, Section B.2.8.5.
- For more information on service-related items, please see:
    - EIS contract Section B.2.10 Service Related Equipment
    - EIS contract Section B.2.11 Service Related Labor
- Please refer to a contractor's individual EIS contract for specifics on the contractor's MSS offerings.
- For additional EIS information and tools, visit the EIS Resources Listing.
- For guidance on transitioning to EIS, please visit EIS Transition Training where you'll find several brief video training modules.