2.1.12 Managed Security Service [C.2.8.5]

Our teammate, Raytheon Company ("Raytheon"), provides the Managed Security Service (MSS) to meet the requirements for the EIS program and Foreground, recently acquired by Raytheon, will provide tools and SOC services. Agencies must keep up with today's increasingly formidable cyber threats, as cybercriminals and corrupt organizations grow in sophistication and number. To combat these threats, a combination of automated and human-driven solutions are necessary to establish always-alert, hypervigilant positioning for incident anticipation, discovery, response, and mitigation. Raytheon's MSS provides EIS with Managed Prevention Services (MPS), Vulnerability Scanning Services (VSS), and Incident Response Services (INRS) to safeguard Agency internal networks and systems against ever-evolving security threats.

2.1.12.1 Compliance with Evaluation Criteria [L.29.2.1]

Raytheon's MSS solution fulfills the mandatory service requirements for MSS defined in SOW paragraph C.2.8.5. The following section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.12-1** highlights some key strengths and benefits of our MSS solution.

Exhibit 2.1.12-1. Features and Benefits of the Raytheon Solution

Evaluation Criteria	Features and Benefits of Raytheon's Approach
Understanding (M.2.1(1))	• The requirements outlined in the SOW correspond with the MSS Raytheon has provided to multiple Government Agencies. • Raytheon has integrated managed prevention solutions into multiple Government Agencies (cited in QOS below) and commercial clients and monitors the installed solutions via the Raytheon Virtual SOC (V-SOC) in Herndon, Virginia. • Raytheon has successfully applied [redacted] in analyzing and reporting the security posture of client computer and network environments qualitatively and quantitatively improving their security posture • Raytheon's incident response programs are developed and integrated into the client business operations and have been at the forefront of remediating large scale agency and industry breeches
Quality of Services (M.2.1(2))	• Raytheon's extensive Government support has allowed us to tailor our MSS approach for supporting [redacted]

Evaluation Criteria	Features and Benefits of Raytheon's Approach
	[redacted] and for large scale cloud environments such as the [redacted] etc. • These Government Agencies have provided us with numerous commendations and excellent reviews when directly interacting with key Government Agency personnel.
Service Coverage (M.2.1(3))	• MetTel provides MSS in the top [redacted], CONUS, and OCONUS.
Security (M.2.1(4))	• Raytheon delivers remote managed services [redacted] • We access [redacted] • Raytheon utilizes a [redacted] • Our blended MSS team comprises experienced TS/SCI cleared analysts and engineers who are available as "smart hands" to support DHS supplied equipment. • The MSS team works in concert with our NOC and is [redacted]

2.1.12.1.1 Service and Functional Description [L.29.2.1, C.2.8.5.1, C.2.8.5.1.1]

Raytheon's MSS [redacted] The tools utilized by our MSS include, but are not limited to, [redacted] Our MSS model automates much of the signature-based network security tools through our patented [redacted]

Our MSS offering includes the following benefits on a 24x7x365 basis:

- Security monitoring and analysis support to investigate threats identified through our MPS, VSS, and INRS
- Full management, content development, integration, and engineering key security tools including Agency edge routers
- Active advanced detection and threat "hunting" through a combination of our [redacted]
- DFIR support for compromised systems and network attacks

As depicted in **Exhibit 2.1.12-2**, Raytheon's MSS ties the MPS, VSS, and INRS together into a living and breathing lifecycle that continually increases the MSS's human and machine learning and its overall capability to protect against security threats. The products (output) of one service are ingested into the other services for validation. [redacted]. **Exhibit 2.1.12-3** shows the metrics displayed on the client interface of [redacted]

Exhibit 2.1.12-2. Raytheon's MSS

Exhibit 2.1.12-3. Raytheon's [redacted] Client Interface

Raytheon provides the services to design, implement, sustain, manage and monitor diverse MPS systems and components that secure department and agency infrastructures. Our MPS model is further designed to provide all inputs, data points, and updates necessary to support an enterprise incident management capability. We work with Agency staff [redacted]

Raytheon's VSS model is designed to [redacted] Risks are evaluated according to requirements for compliance as determined by Agency standards. VSS also detects [redacted] We examine the [redacted] We then [redacted] Information from VSS is fed back [redacted]

Raytheon's INRS model is designed to [redacted] We understand the complexities of how to skillfully navigate in

"crisis mode." We integrate with Agency POCs to [redacted] We perform [redacted] to ensure incidents are not repeated.

The [redacted] platform [redacted] Content from [redacted] investigations or incidents [redacted] to support enterprise workflow.

Once the determination has been made that an incident is occurring or has occurred, our analysts [redacted] Understanding where and when to utilize these standard Agency processes is a major part of [redacted]

[redacted]

Exhibit 2.1.12-4. ATIP Interface

2.1.12.1.2 Standards [L.29.2.1, C.2.8.5.1.2]

MSS complies with all the appropriate standards for any underlying EIS access and transport service and the specific standards and requirements identified in an Agency Task Order as required in C.2.8.5.1.2.

2.1.12.1.3 Connectivity [L.29.2.1, C.2.8.5.1.3]

MSS connects to and interoperates with the Agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the Agency. MSS also supports connectivity to Extranets and the Internet and ensures seamless connectivity to Agency networking environments as specified in C.2.8.5.1.3.

2.1.12.1.4 Technical Capabilities [L.29.2.1, C.2.8.5.1.4]

Raytheon's team leverages an integrative approach to develop and provide MPS, VSS, and INRS. Our MSS fuses [redacted]

We [redacted] referenced in **Exhibit 2.1.12-5**.

Exhibit 2.1.12-5. Raytheon's MSS Flow

Custom content is what drives the advanced capabilities offered in our Security Analytics. Our team maintains

2.1.12.1.4.1 Managed Prevention Service (MPS) [C.2.8.5.1.4.1]

In support of MPS, the Raytheon team provides enterprise As part of our MPS turnkey capability, Raytheon Security Engineers These components are designed and rigorously tested to meet, or exceed, network performance KPIs and Agency functionality requirements. Following design and testing, our team the appropriate Agency-specific data. As part of on-going management, in accordance with our focus on continuous service improvement, our team

[redacted] are the core of the successful SOC and MSS business we provide to numerous Federal Agencies. Our team [redacted] Raytheon maintains a [redacted]

Our management approach is aligned to industry best practices such as ITILv3 for Service Management. This approach guides MPS and dictates rigorous testing and deployment processes, detailed outage reporting and root cause analysis, and continuous service improvement. At a tactical level, Raytheon's staff [redacted]. Finally, we make available to the Agency all service related data including, but not limited to, [redacted]

2.1.12.1.4.2 Vulnerability Scanning Service (VSS) [C.2.8.5.1.4.2]

Raytheon's MSS uses a standard, [redacted] (shown in **Exhibit 2.1.12-6**) for our VSS that tests [redacted]

[redacted]

Exhibit 2.1.12-6. Raytheon's Four Phase Vulnerability Testing Methodology

Scoping

Scoping involves gathering general information (see **Exhibit 2.1.12-7**) via the following sources and methods:

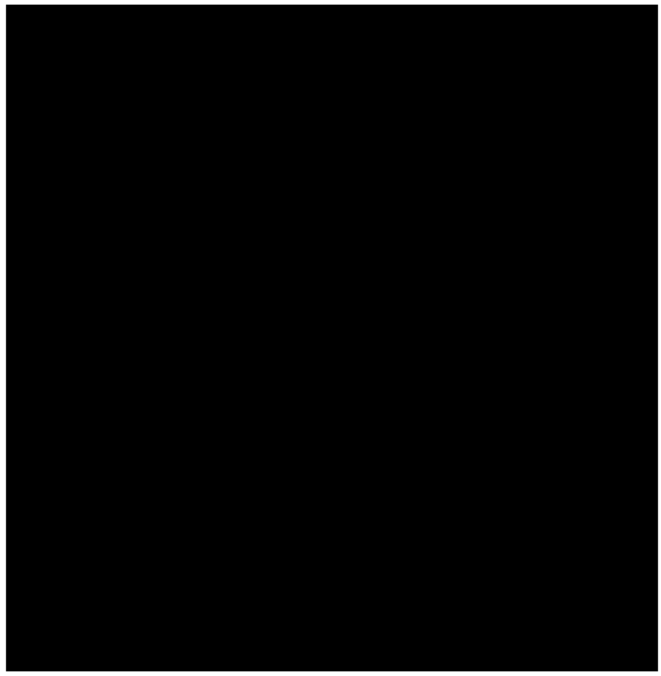


Exhibit 2.1.12-7. Scoping

Reconnaissance

This phase consists of profiling the target environment (see **Exhibit 2.1.12-8**) and . Some of the steps taken in this phase of target discovery and target enumeration include:

Exhibit 2.1.12-8. Profiling Target Environment

[redacted]

Multiple commercial and open source tools may be used during this phase, including those listed in **Exhibit 2.1.12-9** commonly used by Raytheon:

Exhibit 2.1.12-9. Commonly Used Tools

[redacted]

Testing

In this phase, the MSS analysts [redacted] In cases where an individual finding has an exceptionally large number of potentially affected hosts, [redacted] **Exhibit 2.1.12-10** displays some of the key components to the Raytheon testing phase. The MSS analysts:

[redacted]

Exhibit 2.1.12-10. Testing Phase

[redacted]

In the event of a test with rules of engagement permissive to exploitation, [redacted]

[redacted]

Reporting

The reporting phase shown in **Exhibit 2.1.12-11** proactively notifies the agency of [redacted] with the Agency's own risk acceptance policy. The reports create a clear understanding and correlation of:

[redacted]

Exhibit 2.1.12-11. Reporting Phase

[redacted]

Risk Assessment

During the activation phase, a [redacted] to define [redacted] are detected. The Raytheon team works with the Agency to [redacted]

2.1.12.1.4.3 Incident Response Service (INRS) [C.2.8.5.1.4.3]

Raytheon's MSS Incident Response Service provides [redacted] that are key to the Agency's continued cyber security success.

Incident Response Preparation and Planning

The most successful incident response programs are developed and integrated into business operations well in advance of a security incident. As part of the INRS, Raytheon MSS [redacted]

Raytheon's MSS also provides an [redacted]

Incident Response and Management Services

Under the INRS, Agencies receive priority access to Raytheon's MSS analysts and Subject Matter Experts (SMEs). Key elements of this support include:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

When a potential security incident is identified, Raytheon's MSS SMEs [redacted]

[redacted] to minimize exploitation of Agency assets. [redacted] Our MSS team [redacted] the successful remediation of any vulnerabilities.

Our MSS INRS team [redacted], subject to direction by authorized Agency personnel. The Agency may request documentation and case notes at any stage of this response process.

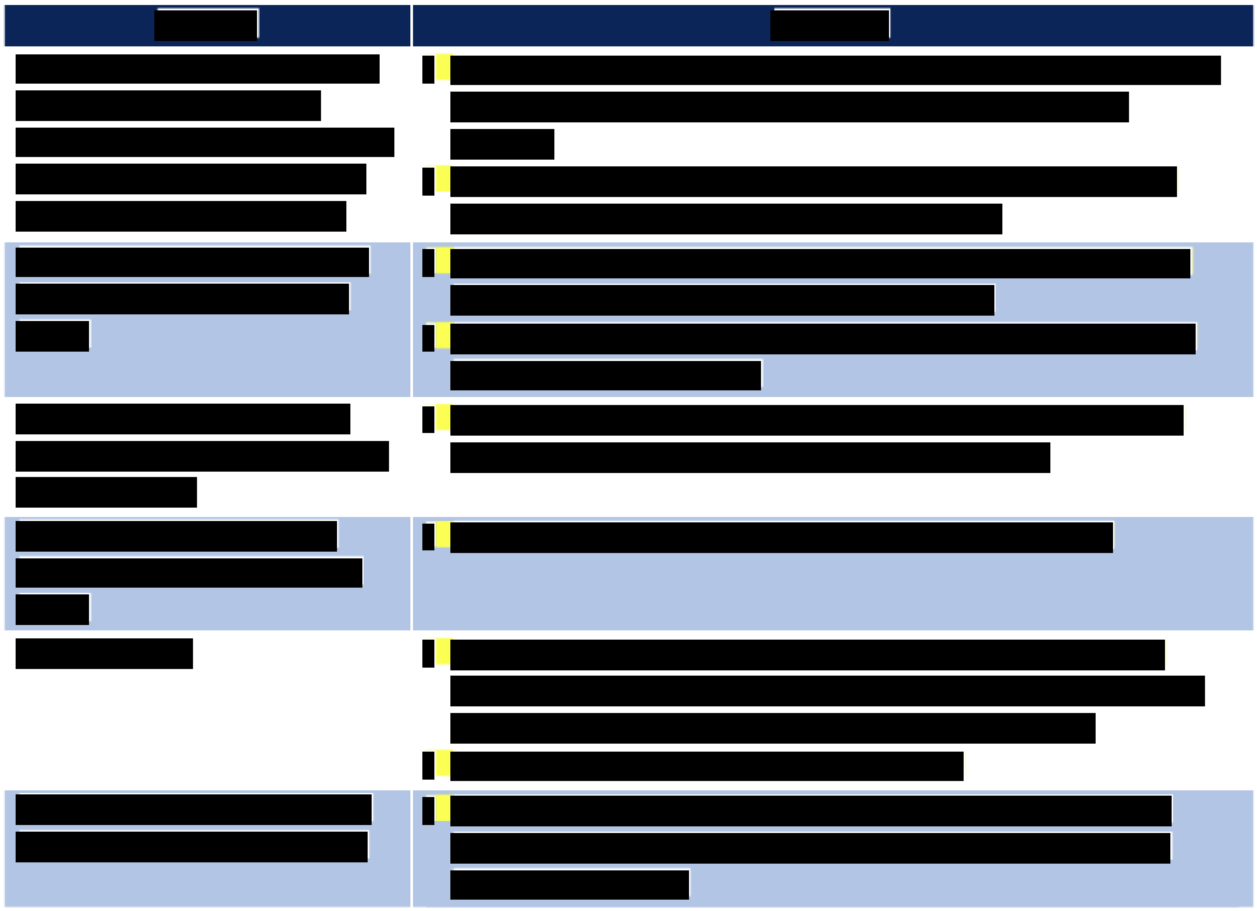
Service Level Objectives

For the INRS, Raytheon's MSS SLA objective is a [redacted]

Core Capabilities

Our activities are performed in such a manner to [redacted] **Exhibit 2.1.12-12** lists key INRS capabilities.

Exhibit 2.1.12-12. Raytheon INRS Capabilities



As part of Raytheon's MSS, we act as part of the Agency's [redacted] Our incident reporting includes [redacted]

From the time of discovery, [redacted] provide the Agency team the ability to trace each incident response lifecycle and participate [redacted]

To facilitate [redacted] Each of the content elements denoted under each step of the incident handling methodology play a critical role in said incident handling methodology detailed in **Exhibit 2.1.12-13**. Our team [redacted]

[redacted]

Exhibit 2.1.12-13. Raytheon INRS Handling Methodology

2.1.12.1.5 Features [L.29.2.1, C.2.8.5.2]

Raytheon's MPS provides the features listed in **Exhibit 2.1.11-14**.

Exhibit 2.1.12-14. Raytheon MPS Features

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Raytheon's MSS [redacted] as requested by the Agency and [redacted] One of the differentiating

factors for Raytheon's VSS is [redacted]

Raytheon's advanced INRS has played a key role in the Federal and commercial space for active attacks; [redacted] Our seasoned INRS personnel have [redacted] methods for uncovering evidence of compromise or validating false positives do not change and are [redacted] While not analyzing during an active incident, [redacted]

2.1.12.1.6 Interfaces [L.29.2.1, C.2.8.5.3]

The Raytheon MSS supports the interfaces of [redacted]

2.1.12.1.7 Performance Metrics [L.29.2.1, C.2.8.5.4]

We meet or exceed the values of the KPIs for MSS and all underlying EIS security services we manage.

Raytheon supports all performance metrics for our MSS as specified in the Task Order. In addition to the MetTel EIS Portal, the [redacted]