2.1.14 DHS Intrusion Prevention Security Service [C.2.8.9]

The Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C), is partnering with select Internet Service Providers (ISP) to provide support for the Einstein 3-Accelerated (E3A) program. The E3A program provides protection from Advanced Persistent Threats (APT) to Internet traffic either destined to, or originating from federal civilian Executive Branch participating Departments and Agencies (PA), commonly referred to as ".gov" traffic. The Intrusion Prevention Security Service (IPSS) is at the core of the E3A program; providing the integrated cyber appliances needed to meet E3A objectives.

MetTel IPSS

- Compliant, scalable, reliable, and resilient solution
- Incremental IPSS implementation capability
- Extens ble approach to add future DHS EINSTEIN Enclave features

The MetTel IPSS solution fulfills the mandatory service requirements for the IPSS in SOW paragraph C.2.8.9. It will provide a continuous monitoring environment including the application of intrusion prevention capabilities of Participating Agency approved agency traffic. The service will be based upon guidance received from the U.S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD), Director of National Intelligence, NIST, industry standards, and MetTel best practices. Additionally, the IPSS extensible environment can be enhanced in compliance with future developments as they evolve.

Upon becoming an MTIPS provider, MetTel intends, with DHS approval and support, to participate in the Einstein program as a provider. With the assistance of Raytheon Company (Raytheon), we will establish an accredited TS/SCI Sensitive Compartmented Information Facility (SCIF) E3A Enclave and implement the functions of the E3A program for the IPSS capability. The MetTel Team offers an expandable and extensible architecture capable of providing all capabilities identified in the 5 March 2013 IPSS Statement of Objectives (SOO).

[redacted]

[redacted]

[redacted]

2.1.14.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel IPSS solution fulfills the mandatory service requirements for IPSS in C.2.8.9. It is nominally sized to support 10 Gbps throughput. This section presents a technical description of our offering and demonstrates our capabilities in Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Security. **Exhibit 2.1.14-1** highlights some key strengths and benefits of our IPSS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.14-1. Features and Benefits of Approach to IPSS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• MetTel's teammate Raytheon, a cybersecurity leader for more than 30 years, developing and deploying technologies that keep Enterprises through Nation States attacks safe. Raytheon has expanded their industry-leading capabilities through over $5 billion invested in 17 acquisitions in the past ten years. Its focus on Cyber Security has made it a worldwide leader in defensive cyber security systems. • Intranet, Extranet, and remote access using industry-standard protocols such as IPsec and TLS across properly sized access methods. • Secure VPNs that are based on IPSec, cryptographic algorithms, and industry-standard authentication methods and that transverse trusted VPNs or Internet Protocol Service (IPS) • Architecture is extens ble to enable new protocols.
Quality of Services (M.2.1(2))	• Full compliance with all SOW performance metrics including performance metrics specified in future task orders

Evaluation Criteria	Features and Benefits of MetTel's Approach
	• Scalable architecture enables addition of future capabilities [redacted] • Resilient – The IPSS components that comprise the IPSS are designed to fail open (no blockage of data)
Service Coverage (M.2.1(3))	• None, RFP Section B.1.2.1.1, Pricing Identification Structure specifies CBSA does not apply to IPSS.
Security (M.2.1(4))	• IPSS operates within a secure environment that assures availability, confidentiality, and integrity of the network traffic being monitored and processed. • Compliance with the IPSS Security Requirements Traceability Matrix (SRTM) that are derived from NIST SP 800-53v4. • IPSS components are designed to fail "open"; no data is prevented from passing through. • [redacted]

2.1.14.1.1 Functional Description [L.29.2.1, C.2.8.9.1, C.2.8.9.1.1]

[redacted]

Functional System Design Overview

[redacted]

Assumptions

[redacted]

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

Core Infrastructure

[redacted]

[redacted]

Core Infrastructure IPSS Concept of Operations

Per the IPSS requirements, we provide the ability to capture and store packet and other analytically relevant data. [redacted]

[redacted]

[redacted]

[redacted]

Alerting and Reporting

[redacted]

[redacted]

[redacted]

Overall, Raytheon’s Core Infrastructure Service solution meets all DHS and MetTel requirements while providing flexibility to expand to a highly available architecture and integrate future capabilities.

Performance Specification

Initial design capacity is driven by PA service level agreements (SLA). Latency (DNS) is dictated by system processing latency and physical displacement. [redacted]

System Design Detail

This section provides a detailed overview of our solution, describing each component and its function. All components were selected after detailed trade studies.

Firewall

[redacted]

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

[redacted]

Event Logging Event Capture & Storage

[redacted]

System Monitoring

[redacted]

DNS IPSS Concept of Operations (Blocking, Sink-holing)

[redacted]

[redacted]

[redacted]

DNS Detection/ DNS Alert Response / Blocking / Sinkhole

[redacted]

- [redacted]

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

[redacted]

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

[redacted]

E-Mail (SMTP) Processing

[redacted]

[redacted]

[redacted]

[redacted]

Secure Environment

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Indicator and Signature Management

[redacted] development and approval.

2.1.14.1.2 Standards [L.29.2.1, C.2.8.9.1.2]

MetTel's partner, Raytheon, is a commercial service provider participant in the DHS Enhanced Cybersecurity System (ECS) program. Performance and security requirements and standards are similar to IPSS. Raytheon's experience will be leveraged to expeditiously implement IPSS.

Applicable Regulations, Policies, and Instructions

MetTel understands the importance of providing a fully compliant system that not only adheres to government standards but also provides assurance that information security and privacy concerns remain paramount. Our solution ensures a low-risk transition to operations based on the current version of NIST SP 800-53v4, “Recommended Security Controls for Federal Information Systems,” the current version of NIST SP 800-37, NIST SP 800-64 “Security Considerations in the Information System Development Life Cycle,” and FIPS PUB. In addition, [redacted]

Verification & Validation

Verification and validation is subdivided into three categories: *Developmental* which confirms correct implementation of a new capability; *Assessment and Accreditation* which confirms the security and hardening of the IPSS; and *Operational* which confirms the correct functioning of signatures and indicators within the IPSS. DHS NCSD and DHS I&A are invited to observe or participate in any developmental capability testing or operational signature testing. Test reports will be available for review and concurrence.

Developmental

With each increment of the component integration and configuration, testers, independent of the network engineer, will conduct component or product-level testing. The testers will create test cases that are traceable to all requirements in the system specification and SRTM. Once a network engineer completes and verifies a requirement, the designated tester will develop and execute a test case. As new functionality is added to the baseline, the tester performs regression tests to ensure that newly integrated capabilities do not affect existing functionality. Any discovered non-conformances will be entered into the defect tracking tool, fixed by the development team, and validated by the tester. The testers will also create test data sets and configure the test harnesses as required to allow verification of all requirements.

MetTel is responsible for injecting the test data sets into the systems under test. If any non-conformances are discovered, they will be documented and fixed by the technical team in order to complete checkout verification.

Assessment & Authorization

Following verification of functionality, a Raytheon and MetTel technical team will prepare the system for acceptance test and assessment and authorization (A&A) activities. Raytheon will assist MetTel to provide inputs to a set of security artifacts that are used by the government to assess the security posture of the services provided by the contractor. This includes, but may not be limited to: Security Concept of Operations (SECONOPs), an Architectural overview, Standard Operating Procedures (SOP), System configurations for all devices performing security-relevant functions, including configurations of all security-related software, an SRTM Response, Vulnerability and penetration test results, incident reports (or templates) used to detail any security incidents already experienced on the system, and if applicable, source code for custom code developed, including modifications to commercial or open-source programs, and a Plan of Action and Milestones (POA&M) that identifies security findings and associated plans to remediate those findings.

Typical preparations include clearing out all logs, and configuring the system to a candidate set of PA parameters that MetTel has agreed to with DHS for acceptance testing. The Raytheon technical team will perform dry runs of the acceptance test cases to ensure the IPSS system is ready for acceptance testing.

In support of the certification and accreditation, Raytheon will support technical assessments including testing of controls, system penetration testing, and security compliance reviews and audits. We will also support development of mitigation plans for open findings. This phase ends when the IPSS systems have been accredited and MetTel has received an ATO.

Operational

As part of the IPSS delivery, MetTel will provide a Service Verification Environment (SVE). The SVE complements the operational IPSS and is a form-fit-function identical instantiation of the IPSS. The purpose of the SVE is to confirm the proper functionality of signatures under simulated, representative traffic prior to upload to the IPSS.

2.1.14.1.3 Connectivity [L.29.2.1, C.2.8.9.1.3]

[redacted]

[redacted]

2.1.14.1.4 Technical Capabilities [L.29.2.1, C.2.8.9.1.4]

Exhibit 2.1.14-5. Required Technical Capabilities

Requirement	Response
1. Establish and support a process that allows DHS to provide cyber threat indicators and define desired effects in the protection of covered network traffic.	[redacted]
2. Demonstrate to DHS that IPSS operates as intended when traffic is present that matches malicious indicators prior to the activation of new or modified indicators and their associated actions.	[redacted]
3. Support a process that allows DHS to direct actions on network traffic to gather additional information on cyber threats, stop cyber attacks, and/or respond to cyber incidents.	[redacted]
4. Provide for the ability to receive, accept, utilize, and secure GFI up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level, including PII, such as cyber threat indicators signatures, and associated actions in accordance with DHS-approved security guidelines.	[redacted]
5. Provide an automated means for DHS to share GFI and utilize the GFI provided within the DHS IPSS in as near real-time as poss ble.	[redacted]
6. Establish or leverage additional commercially available cyber threat information and/or DHS IPSS functional capabilities to provide additional protections for Federal Systems.	[redacted]
7. Ensure only those indicators and associated	[redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Requirement	Response
actions that are approved and further specified by DHS are applied to Participating Agencies.	[redacted]
8. Provide the ability to apply different sets of mitigation capabilities to a Participating Agency's traffic that does not affect which mitigations are applied to a separate Participating Agency's traffic.	[redacted]
9. Ensure that GFI is not disclosed or shared with any third party or used for any purpose that DHS has not specifically authorized.	[redacted]
10. Gain access to approved Participating Agency Federal System network traffic that uses the contractor as its Internet service provider.	[redacted]
11. Establish the ability to detect malicious network traffic to support the DHS IPSS and to provide additional contextual information associated with alerts to support post-incident analysis	[redacted]
12. Support signature-based, heuristic-based and/or other emerging detection methods.	[redacted]
13. Provide solutions that allow for the detection of malicious activity within encrypted traffic.	[redacted]
14. Support a wide-range of unclassified and/or classified protection measures. The kinds of protection measures the government expects to be available via a DHS IPSS can best be described by referencing the NIST Guide to Intrusion Detection and Prevention Systems. The guide defines typical IPSS capabilities as providing the capability to: • collect more detailed information for a specific	[redacted]

Requirement	Response
session after malicious activity has been detected	[redacted]
• prevent or block a detected threat by terminating the network connection or blocking access to the target	
• change the attack's content by removing or replacing malicious portions of an attack to make it inoperable	
• see evasion techniques and duplicate processing performed by a target	
• tune detection accuracy so that an organization can achieve an optimum mix of false positives to false negatives in line with that organization's risk tolerance	
15. Include the ability to redirect to a safe server.	[redacted]
16. Allow for the capturing and storing of analytically relevant data associated with potential harmful network traffic specific to some indicators but and not necessarily applied to all indicators.	[redacted]
17. Ensure that the DHS IPSS technology does not retain traffic other than traffic associated with suspected malicious activity or as otherwise required by DHS.	[redacted]
18. Apply DHS-directed prevention services, as defined and approved by the United States Computer Emergency Readiness Team (US-CERT).	[redacted]
19. Apply DHS-directed prevention services through an approved traffic segregation solution to only designated, Federal System network traffic.	[redacted]
20. Operate as an in-line service (i.e., a service within the ISP network boundary that is capable of performing mitigation actions as traffic traverses the ISP network in the normal flow of traffic) that detects and mitigates malicious IP-based traffic. For the purposes of this contract and to maximize contractor flexibility, the term "in line" should not be construed as mandating a specific network architecture, rather, the service should ensure that the following two conditions are met:	[redacted]
a) All Internet traffic delivered to the Participating Agency's SDP shall be monitored and subject to mitigation by the Prevention Service prior to said delivery.	[redacted]
b) All Participating Agency traffic delivered to the	[redacted]

Requirement	Response
Internet via the Participating Agency's SDP shall be monitored and subject to mitigation by the Prevention Service prior to said delivery.	[redacted]
21. Define and apply the full range of existing and future DHS IPSS functional capabilities (typically defined in a technology roadmap) at cyber-relevant speed to counter cyber threats and attacks.	[redacted]
22. Provide quarantined malware to Participating Agency and to DHS via the US-CERT malware lab or other specified DHS entity.	[redacted]
23. Prior to utilization of cyber threat indicators, signatures, and/or countermeasures, demonstrate to the government that cyber threat indicators, signatures, and/or countermeasures provided operate as intended.	[redacted]
24. Provide DHS and Participating Agencies with detection alerts and associated contextual information around suspicious traffic sufficient to identify the facts of a particular incident or attempted incident for protected traffic in accordance with DHS specifications or guidance.	[redacted]
25. Provide DHS and Participating Agencies with data to support network traffic pattern assessments to detect and address anomalous patterns that may be indicators of malicious activity in accordance with DHS specifications or guidance.	[redacted]
26. Provide DHS and Participating Agencies with information related to indicators, signatures, associated actions, and/or alerts over a given time period.	[redacted]
27. Ensure that agency network traffic and other information are not disclosed to any party other than DHS and the agency and then only as specifically identified under this contract and task orders thereto, and take necessary steps to ensure Participating Agency data is secure from unauthorized access, use, disclosure, or retention.	[redacted]
28. Provide test results and support a process that allows for government participation and observation in tests.	[redacted]
29. Within 15 minutes of discovery, notify DHS of any unauthorized access, use, disclosure, or retention of Participating Agency data, and of any breach of any	[redacted]

Requirement	Response
security or information handling requirements or additional instructions provided by DHS regarding the handling of Participating Agency network traffic, and provide relevant information to allow DHS to assess the scope of any such breach.	[redacted]

2.1.14.2 Features [L.29.2.1, C.2.8.9.2]

[redacted]

2.1.14.3 Interfaces [L.29.2.1, C.2.8.9.3]

[redacted]

2.1.14.4 Performance Metrics [L.29.2.1, C.2.8.9.4]

The representative architecture in this section is designed to be modified to meet latency, capacity, availability, reliability, and protocol metrics as defined in individual TO.