VOLUME 1, SECTION 5.3: INTRUSION DETECTION AND PREVENTION SERVICE

5.3 INTRUSION DETECTION AND PREVENTION SERVICE [C.2.10.2, M.2.1.3]

The Level 3 Team's Intrusion Detection and Prevention Service (IDPS) will meet or exceed the Government's requirements for IDPS, as defined in RFP Section C.2.10.2. This section provides a description of our service offering followed by responses to the specific requirements listed in RFP Section L.34.1.6.

Level 3's IDPS solution will support agencies with trained security experts who can determine whether an event needs to be investigated and stopped, or whether the traffic is normal. This solution will protect agency networks and servers from over [redacted] attacks and malicious code. Features are highlighted below.

[redacted]

[redacted]

Through our IDPS solution, Government agencies will benefit from fast and simple deployments, updates, and configuration because the same underlying technology drives the various agents. The result will be reliable threat detection, prevention, and response that truly protects while enabling electronic business continuity and integrity. By outsourcing IDPS, agencies can focus on their core competency and be assured that security experts are watching their networks for malicious traffic, worms, and spyware [redacted].

5.3.1 Technical Approach to Security Services

This section addresses the requirements contained in RFP Section L.34.1.6.1 as they apply to our IDPS offering. The topics covered include the Level 3 Team's approach for Service Delivery, our approach regarding Federal agency Enterprise Architecture objectives, and any foreseen problems and solutions related to our offering.

5.3.1.1 SERVICE DELIVERY

Level 3's Service Delivery objective is to provide Government agency customers with rapid and responsive service delivery for our Intrusion Detection and Prevention Services. All services proposed by the Level 3 Team for [redacted] will use the same Service Delivery process. Level 3's Networx delivery process is discussed in detail in Section 3.1.1.1 of this proposal volume.

5.3.1.2 FEDERAL AGENCY ENTERPRISE ARCHITECTURE

The method for addressing the FEA objectives for our agency customers under (3)Enterprise is independent of the service being procured. Section 3.1.1.2 of this proposal volume contains a detailed discussion of the Level 3 Team's proposed approach for FEA.

5.3.1.3 FORESEEN PROBLEMS AND SOLUTIONS

The Level 3 Team has reviewed the individual service requirements for IDPS in RFP Section C.2.10.2.1.4. Our solution complies with all of the requirements. Our IDPS systems include automatic patch management/virtual patch management capabilities and signature updates to protect itself and the network from known vulnerabilities.

5.3.2 SATISFACTION OF SECURITY SERVICES PERFORMANCE REQUIREMENTS [C.2.10.2.4]

This section addresses the requirements contained in RFP Section L.34.1.6.2 for the Level 3 Team's Quality of Service. The topics covered are quality of services with respect to performance metrics, monitoring and measuring Key Performance Indicators (KPI) and Acceptable Quality Levels (AQL), testing procedures, and proposed performance improvements and associated benefits.

5.3.2.1 QUALITY OF SERVICE

[redacted]

5.3.2.2 MONITORING AND MEASURING KPIS AND AQLS

The Level 3 Network Operations Center will monitor all Networx services provided using our IP back bone. Section 3.1.2.2 of this proposal volume describes the monitoring tools used by this organization that will allow for comprehensive visibility of numerous network elements and the ability to accurately measure AQLs for the applicable KPIs.

The KPIs measured for IDPS are described below.

[redacted]

5.3.2.3 KPI AND AQL COMPLIANCE

Please see the response to Section 2.2.3 for a discussion of the management expertise and toolsets used by Level 3 to ensure KPI and AQL compliance.

5.3.2.4 PROPOSED PERFORMANCE IMPROVEMENTS

Level 3 does not intend to exceed the AQLs in the KPIs at this time but would like to reserve the ability to do so with performance improvements that may be attained through the introduction of new technology. Level 3 believes in continuous improvement and will always strive to provide the highest quality services available.

5.3.2.5 PROPOSED PERFORMANCE METRICS

The Level 3 Team will not propose additional performance metrics for our IDPS offering at this time.

5.3.3 Satisfaction of Security Services Specifications

This section demonstrates the Level 3 Team's ability to satisfy the service requirements for IDPS. We also describe anticipated modifications to the network for delivery of the service and our experience delivering the service.

5.3.3.1 SERVICE REQUIREMENTS

Level 3's Intrusion Detection and Prevention Service offering fulfills the Mandatory Service Requirements for IDPS contained in RFP Section C.2.10.2.1. This section demonstrates our capabilities in the following areas:

- Standards
- Connectivity
- Technical Capabilities
- Features
- Interfaces

5.3.3.1.1 Standards [C.2.10.2.1.2]

Level 3's IDPS complies with the required standards as delineated in RFP Section C.2.10.2.1.2. Members of our team are active in numerous industry forums and working groups, which demonstrates our commitment to implementing future standards as technologies are developed and standards are defined and become commercially available. Our memberships include:

- Intrusion Detection Exchange Format Working Group (IDWG)
- Network Service Provider Security Association (NSP-Sec)
- International Systems Security Association (ISSA)
- VoIP Security Association (VOIPSA)
- Intrusion Detection Systems Consortium
- National Infrastructure Advisory Council (NIAC)
- Department of Homeland Security (DHS)
- National Institute of Standards and Technology (NIST)
- National Information Assurance Partnership (NIAP)

- Federal Bureau of Investigation (FBI)
- National Association of State Chief Information Officers (NASCIO)
- Information Technology - Information Sharing and Analysis Center (IT-ISAC)
- Open Security Evaluation Criteria (OSEC)

5.3.3.1.2 Connectivity [C.2.10.2.1.3]

Level 3 is a Tier 1 Internet Service Provider. Our IDPS offering meets the connectivity requirements listed RFP Section C.2.10.2.1.3.

5.3.3.1.3 Technical Capabilities [C.2.10.2.1.4]

Our IDPS solution complies with the 31 mandatory requirements listed in RFP Section C.2.10.2.1.4. Details follow.

Provide design and implementation services

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Level 3 will provide the necessary hardware and if necessary, software. The basic platforms that support our IDPS offering are described below.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Subscribing agencies can use the [redacted] portal to report and/or obtain status information for ongoing events in real time. [redacted]

The IDPS devices that will enable our solution have the ability to proactively block threats before they affect the network; however, these devices cannot fix a vulnerability, which typically involves patching a vulnerable system.

Level 3's IDPS systems include [redacted]

Enabled by this feature, the IDPS devices and a security analyst have the ability to take the following actions to respond dynamically and take proactive and corrective actions:

[redacted]

Upon notification of an attack, the Level 3 Team will respond and also offer remediation recommendations to the affected agency.

Employ defense mechanisms to detect and accurately stop attacks:

[redacted]

[redacted]

The Level 3 Team's solution includes [redacted] support from a dedicated agency Help Desk. Details on this Help Desk function are provided in Section 5.1.3.1.3.4. Our Help Desk will coordinate with the [redacted] to notify agencies of events based on [redacted]. The Help Desk will also provide [redacted] which may include [redacted]

The [redacted] portal will provide agencies with the necessary means to provide analysis and interpretation of the attack data. This includes access to raw and normalized log files, event escalation information, reports, and other information that will help the agency understand the attack. [redacted] analysts will also be available to discuss any security incidents that were escalated to the agency.

The Level 3 Team will communicate with the IDPS device through a variety of methods. All methods of communication involve one or more of the following:

[redacted]

Level 3 will work with the agency to determine the most suitable method for the agency's deployment.

The [redacted] portal will provide agencies with [redacted] access to the information below, and much more:

[redacted]

[redacted]

[redacted]

[redacted]

Section 5.2.3.1.3.4 of this proposal volume discusses Level 3's procedures for configuration changes.

Test and deploy the latest patches and bug fixes:

[redacted]

Prior to deploying any patches onto an agency's device, Level 3 will test all patches and bug fixes to ensure the patch does not cause any harm to the agency's environment.

Testing at Level 3 is given great importance in the engineering and operations processes. It is continuously performed in Level 3's own extensive laboratory facilities. Details on this laboratory and our testing procedures are provided in Section 2.3.3 of this proposal volume.

Maintain the latest configuration information for restoration purposes:

All device configuration information, including IDPS policies, is available online, through the [redacted] portal, for agency verification. We also maintain this information internally at our [redacted] to enable service restoration in the event of a device failure.

Perform periodic security scans capable of revealing system vulnerabilities:

[redacted]

Document the results of the scans and the solutions:

All scan results will be posted to the [redacted] portal. The results will also be archived for [redacted]

Support networks of varying complexity:

[redacted]

5.3.3.1.4 Features [C.2.10.2.2]

There are no features specified for IDPS.

5.3.3.1.5 Interfaces [C.2.10.2.3]

As applicable, Level 3's IDPS offering will support the UNIs defined in the following sections of the RFP:

[redacted]

5.3.3.2 PROPOSED SERVICE ENHANCEMENTS

The Level 3 Team does not propose service enhancements to IPDS at this time. As new FISMA compliant features and functionality are added to the chosen platform Level 3 will work with the agency to roll out the new features and functionality.

5.3.3.3 NETWORK MODIFICATIONS

The Level 3 Team anticipates the need for very minimal modifications to the network for delivery of IDPS, with negligible impact on the security or performance of the network.

The Level 3 Team does not anticipate the need for any major modifications to the network for delivery of IDPS. We will require the agency to open ports on their Internet facing firewall to allow the IDPS device to communicate with the [redacted] Opening ports on the firewall is an everyday occurrence. Depending on the current configuration, it may not be necessary to open any ports at all. The risk to opening the ports is very minimal. The data going through those ports will be encrypted, which virtually eliminates the chance that someone could intercept and read the data. Depending on the deployment, Level 3 may be willing to consider other options.

[redacted]

5.3.3.4 EXPERIENCE DELIVERING IDPS

The Level 3 Team leads the industry in planning and deploying managed security services for both the commercial and Government sectors. We bring nearly 10 years of experience delivering Managed Intrusion Detection and Prevention Services, which includes IDPS support to a Government agency.

The managed services customer base of [redacted] includes over [redacted]. Our customers range from [redacted].