VOLUME 1, SECTION 5.1:

MANAGED TIERED SECURITY SERVICES

5.1 MANAGED TIERED SECURITY SERVICES [C.2.7.4, M.2.1.3]

Level 3 will support the GSA's Multi-Tier Security Profiles (MTSP) initiative in accordance with Tier-2 – Protected Service specifications. We teamed with one of the world's leading Managed Security Services providers, [redacted], to offer one of the most complete and reliable Managed Security Solutions available. Our solution is designed to meet or exceed the Government's requirements for MTSP Tier 2 service, as defined in RFP Section C.2.7.4.1.1.2. A description of our offering is provided below. Responses to the requirements of RFP Section L.34.1.6 follow.

The Level 3 MTSP Tier 2 solution includes the Help Desk function specified for Tier 1 service, and additional technical and management components to support security needs of Sensitive but Unclassified (SBU) mission functions and information. Our Managed Tiered Security Service (MTSS) offering will provide a vehicle for agencies to order individual managed security services a la carte or in a bundle. The components include:

[redacted]

[redacted]

Agencies will gain efficiencies and cost savings through service bundling, versus ordering any of the Managed Security Services a la carte. In addition, there is defense in depth: [redacted]

By subscribing to the Level 3 MTSS offering, agencies will be able to focus on their core competencies while a dedicated Team of trained security experts maintains watch over their networks [redacted] for security violations and maintains certifiable, auditable compliance with applicable FISMA/FIPS requirements.

5.1.1 Technical Approach to Security Services

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

5.1.1.1 Service Delivery

The Level 3 Service Delivery objective is to provide Government agency customers with rapid and responsive service delivery for our Managed Tiered Security Services. All services proposed by the Level 3 Team for [redacted] will use the same Service Delivery process. The Level 3 delivery process is discussed in detail in Section 3.1.1.1 of this proposal volume. We augment this discussion with an overview of our approach to MTSS Deployment, which follows.

MTSS Delivery will require a certified platform(s) (including a selection from supported hardware and software). [redacted]

[redacted]

As a part of the setup, remote management of the platform will be established by [redacted] This connection will provide Level 3 with access to platforms for remote maintenance, troubleshooting and problem resolution. [redacted]

[redacted]

5.1.1.2 Federal Agency Enterprise Architecture Objectives

The method for addressing the Federal Agency Enterprise Architecture (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.

5.1.1.3 Foreseen Problems and Solutions

The Level 3 Team has been setting the standard for accountability, reliability and protection in Managed Security Services arena since [redacted] MTSS is a seasoned service offering and we don't anticipate any problems meeting the service requirements.

5.1.2 Satisfaction of Security Services Performance Requirements

This section addresses the requirements contained in RFP Section L.34.1.6.2 for the Level 3 Team's Quality of Service. We discuss our ability to meet the performance metrics listed for MTSS and our approach for monitoring and measuring Key Performance Indicators (KPI) and Acceptable Quality Levels (AQL); testing procedures; proposed performance improvements; and benefits, rationale and measurement of performance improvements.

5.1.2.1 Performance Metrics [C.2.7.4.4.1]

In accordance with RFP Section C.2.7.4.4 of the RFP, Level 3 will provide the Performance Metrics shown in Table 5.1-1 for our MTSS offering[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]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

5.1.2.2 Monitoring and Measuring KPIs and AQLs

The Level 3 Network Operations Center will monitor all [redacted] services provided using our IP backbone. 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 MTSS are as follows:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted] a required capability for Tier 2 service under the Networx RFP.

[redacted]

[redacted]

[redacted]

[redacted]

5.1.2.3 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.

5.1.2.4 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.

5.1.2.5 Proposed Performance Metrics

Additional performance metrics are not proposed at this time.

5.1.3 Satisfaction of Security Services Specifications

This section addresses the requirements contained in RFP Section L.34.1.6.3 for the Level 3 Team's MTSS offering. We provide a technical description of MTSS and a description of necessary modifications to the network for Service Delivery, our experience delivering MTSS, and our standard approach for securing an MTSS network infrastructure.

5.1.3.1 TECHNICAL DESCRIPTION OF MTSS

The Level 3 Intrusion Detection and Prevention Service offering fulfills the Mandatory Service Requirements for IDPS contained in RFP Section C.2.7.4.1. This section demonstrates our capabilities in the following areas:

- Standards
- Connectivity
- Technical Capabilities
- Features
- Interfaces

5.1.3.1.1 Standards [C.2.7.4.1.2]

The Level 3 MTSS complies with the required standards as delineated in RFP Section C.2.7.4.1.2. Level 3 Team members 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:

- 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)
- Intrusion Detection Exchange Format Working Group (IDWG)

5.1.3.1.2 Connectivity [C.2.7.4.1.3]

Level 3 is a Tier 1 Internet Service Provider. Our MTSS will comply with the connectivity requirements listed RFP Section C.2.7.4.1.3.

5.1.3.1.3 Technical Capabilities [C.2.7.4.1.5]

The Level 3 MTSS solution will meet the requirements of the 15 Security Enhancement Services for Tier 2 Service as shown in the MTSP Security Profile Technical Capabilities Matrix, RFP Section C.2.7.4.1.4.1. Details follow.

5.1.3.1.3.1 Agency Sponsored Type 1 Encryption Service

[redacted]

5.1.3.1.3. Anti-virus Service

The Level 3 AVMS solution will provide [redacted]

[redacted]

5.1.3.1.3.3 Firewall Service

The Level 3 Managed Firewall Service is a comprehensive solution that will allow agencies to outsource daily management and maintenance of their firewalls. The service will include [redacted] management of industry-certified firewall platforms, which will ensure expert monitoring, maintenance and configuration of firewalls at a fraction of the cost required to manage the firewall in-house. Our offering includes [redacted]

5.1.3.1.3.4 Agency Dedicated Help Desk Service

The Level 3 Team provides a state-of-the-art business methodology for handling trouble issues and complaints through [redacted] This model will enable agencies to bypass traditional Tier I type support and direct them to Tier II technical support immediately. This model is fully integrated with a [redacted]

[redacted]

Single Point of Presence

Within the Level 3 [redacted], the [redacted] [redacted] will serve as a single point-of-presence help desk resource for all issues concerning [redacted]

[redacted]

Trouble Detection and Reporting System

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Proactive Monitoring and Opening of Trouble Tickets

Proactive monitoring means that network problems will be discovered by the Help Desk staff before a user is aware of the problem or before the problem becomes significant and affects users. The Level 3 Team’s concept of operations integrates network surveillance with the Help Desk to provide seamless coverage and end-to-end management of all critical network elements. This proactive approach also facilitates the timely update of event status. Level 3 statuses tickets every [redacted] until resolution, at which time the last entry will include the date and time to restore. Trouble tickets will be available [redacted] post resolution. [redacted]

Event Notification

The Level 3 approach to Event Notification includes the following components:

[redacted]

[redacted]

Secure [redacted] Portal

Level 3 provides the Government an insight into the performance of Level 3's proposed Networx services using the [redacted] portal. [redacted]

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

Access to Reports

Agencies will have access to Help Desk reports via the [redacted] portal described above. Level 3 will also accommodate any customer request for report access, such as email or fax, specified by the agency.

Log File and Report Retention

The Level 3 standard archiving procedure calls for storage of system event logs (syslogs) for up to [redacted] for the entire network. [redacted]

[redacted]

5.1.3.1.3.5 Intrusion Detection/Prevention Service

The Level 3 Team’s IDPS solution will support agencies with trained security experts who can determine whether an event is something that needs to be investigated and stopped, or whether the traffic is normal everyday traffic. This solution will protect agency networks and servers from over [redacted]. Features of our offering are highlighted below.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3.1.3.6 Incident Response Service

The Level 3 Team’s Incident Response Service will include an incident response plan that will prepare agencies for and minimize the effects of an information security breach. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3.1.3.7 Network Isolation (Air Gap) Requirements

The Level 3 Team will support the MTSP initiative's Tier 2 – Protected Services requirements. Network Isolation (Air Gap) is not a required capability for Tier 2 service under the Networx RFP.

5.1.3.1.3.8 NSA Approved Multilevel Security Solution

The Level 3 Team will support the MTSP initiative's Tier 2 – Protected Services requirements. NSA-Approved Multilevel Security Solution is not a required capability for Tier 2 service under the Networx RFP.

5.1.3.1.3.9 Packet Filtering Service

The Level 3 backbone has robust packet filtering capabilities. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3.1.3.10 Premises-based VPN Service

Details of our PBIP-VPNS solution and a complete response to RFP Section C.2.7.2 are provided in Section 3.6 of this proposal volume.

[redacted]

[redacted]

The base service for PBIP-VPNS is the Level 3 Internet Protocol Services (IPS). This service is fully described in Section 3.1 of this proposal volume. Our IPS provides [redacted] access for Government agencies. Our world class Tier 1 peering and [redacted] backbone provides a platform that Government agencies can feel secure using to build a VPN. The Level 3 Customer Premises Equipment (CPE) Service Enabling Devices (SEDs) will provide [redacted]

5.1.3.1.3.11 Proxy Server Service

[redacted]

5.1.3.1.3.12 Secure Managed Email Service

Our SMES offering is an [redacted] email solution that will scan all incoming email before it reaches the agency network. As a result of scanning emails for viruses and spam prior to reaching the agency network, all viruses and spam will be blocked before entering the agency network. This will provide the agency with confidence that any spam and viruses will be blocked before they can cause damage to the network.

5.1.3.1.3.13 Security Certification Support Service

Level 3 will perform all tasks required for Security Certification Support. The activities requested are part of the standard services provided by Managed Security Service Providers and is part of the standard operating practices of Level 3's Managed Security Services and that of our subcontractors. Any requirements or tasks specifically related to FISMA compliance are included as part of Level 3's Federal Security Management Program by default. Due to Level 3's participation in the [redacted]

5.1.3.1.3.14 Security Maintenance Service

As required by FISMA, all systems, personnel, facilities, major applications, etc. associated with the Networx Enterprise Program, that are not part of our private sector public services infrastructure (such as IPS), will be subject to the NIST Certification and Accreditation Process as defined in NIST SP 800-37. This is extended to all partner systems, personnel, facilities and major applications that are part of [redacted]. All relevant components, either hosted by Level 3 or our partners, will be integrated into Level 3's Federal Security Management Program and included in the NIST SP 800-18 Security Plan, related risk assessment and the certification process and tested in accordance with NIST SP 800-53A guidelines.

[redacted]

[redacted]

5.1.3.1.3.15 Vulnerability Scanning Service

[redacted]

Our VSS offering will incorporate a high level of flexibility to accommodate the varying needs of all types of agencies—both large and small. In addition, the service will include [redacted] distinct types of scanning that can be employed together or separately:

[redacted]

[redacted]

[redacted]

5.1.3.1.4 Features [C.2.7.4.2.2]

The Level 3 MTSS solution will meet the features requirements in RFP Section C.2.7.4.2, as described below.

5.1.3.1.4.1 On-site Management and Monitoring [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3.1.4.2 On-Site Installation

[redacted]

[redacted] Level 3 will work with agency representatives to ensure that all site equipment needed for a specific deployment is received by the site representative prior to scheduling a site visit for installation.

Local installation subcontractors will minimize risk and limit travel expense. An installation Team of [redacted] persons will be responsible for the following:

[redacted]

[redacted]

[redacted]

5.1.3.1.5 Interfaces [C.2.7.4.3.1]

The Level 3 MTSS will support the User-to-Network-Interfaces (UNIs) at the SDP, as defined in RFP Section C.2.7.4.3.1, for intranet and extranet Connectivity.

[redacted]

The Level 3 Team's MTSS will also support the required UNIs for Remote Access Connectivity, as defined in RFP Section C.2.7.4.3.2.

[redacted]

5.1.3.2 PROPOSED SERVICE ENHANCEMENTS

At this time, Level 3 does not anticipate the need to exceed the specified service required discussed above. As new FISMA-compliant features and functionality are added to any of the proposed platforms, Level 3 will work with agencies to deploy the new features and functionality.

5.1.3.3 Network Modifications

[redacted]

The gateway anti virus component will have minimal impact on the network. The only change to the exiting network will be the need to [redacted] In addition, the service will require a change be made to the agency's [redacted]. This change will have to be done by whoever is providing Domain Name Server (DNS) service to the agency.

Adding a firewall or gateway anti virus solution will decrease the risk to the users of the network, assuming an existing solution isn't already in place. The changes outlined above should have no impact on the user community. In the unlikely event of a problem with the changes during the deployment phase, Level 3 will work with the agency to back out of the deployment. Once any technical issues were resolved, the deployment process could begin again. [redacted]

In-band management is to be performed through [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Our Managed Security Services deployment Team will have access requirements for initial setup of connectivity between the site and the [redacted]

5.1.3.4 Experience Delivering MTSS

Today, more than [redacted] including many leading world governments, all major agencies and departments of the U.S. Federal Government and most U.S. state governments, trust members of the Level 3 Team to protect their critical online assets - across networks, servers and desktops. A few of our more outstanding accomplishments are listed below.

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3.5 APPROACH, PROCESS, AND CONSIDERATIONS FOR SECURING AN MTSS NETWORK INFRASTRUCTURE

This section describes the approach, process and considerations for securing a network infrastructure for MTSS. This response is based on the Level 3 Team's experience with the Tier 2 requirements specified in Section C.2.7.4, and provides a discussion of how our Team would investigate the requirements, design the solution, implement the plan, and deliver service that meets the agency’s performance requirements.

The Level 3 Service Delivery process and our MTSS deployment procedure are described in Section 5.1.2 of this proposal volume. Additional detail on the specific tasks and deliverables that will comprise the process of delivering a compliant and customized MTSS solution is provided below.

Designing a solution for an MTSP Tier 2 Protection system can be accomplished with input and assistance from the subscribing agency. Level 3 would work with the agency to determine how to best secure the infrastructure. This up front consultation will include discussions with key security personnel, review of network diagrams, understanding of current and future needs and concerns, and prioritization of assets and security goals.

The Tier 2 network security requirements call for managed firewalls, managed gateway anti-virus and intrusion detection and prevention service. [redacted]

The upfront assessment will include the following:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Once this assessment is complete, Level 3 will begin deployment of the project, which is a [redacted] process.

5.1.3.5.1 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.1.3.6 Meeting Section 508 Requirements [C.6.4]

Reports generated as a result of an MTSS engagement will be posted on the [redacted] portal. The customer portal meets most of the requirements outlined in Section 508. The Section 508 requirements that are not met today can be met, rather easily, through simple modifications to the portal. Level 3 is committed to making these changes, should they be necessary.

In compliance with Section C.6.4 of the Networx RFP, Level 3 has prepared for a Voluntary Product Assessment Template (VPAT) for MTSS and supporting documentation for Section 508, Subpart B, Technical Standards, paragraph 1194.22, Web-based Intranet and Internet Information and Applications. This data is provided in Section 2.5.5 of this Technical Volume.