VOLUME 1, SECTION 5.7:

SECURE MANAGED EMAIL SERVICE

5.7 SECURE MANAGED EMAIL SERVICE (SMES) [C.2.10.8]

The Level 3 Team's Secure Managed Email Service (SMES) will meet or exceed the Government's requirements for SMES, as defined in RFP Section C.2.10.8. This section provides a description of this service offering followed by responses to the specific requirements listed in RFP Section L.34.1.6.4, as they apply to this service.

Our SMES offering is an outsourced 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.

5.7.3 Service Requirements [C.2.10.8.1]

The Level 3 SMES fulfills the mandatory service requirements defined in RFP Section C.2.10.8.1. This section demonstrates our capabilities in the following areas:

- Standards
- Connectivity
- Technical Capabilities
- Features
- Interfaces

5.7.3.1 STANDARDS [C.2.10.8.1.2]

The Level 3 SMES will comply with the required standards as delineated in RFP Section C.2.10.8.1.2. 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:

- 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)

5.7.3.2 CONNECTIVITY [C.2.10.8.1.3]

Level 3 is a Tier 1 Internet Service Provider. Our SMES offering meets the connectivity requirements listed RFP Section C.2.10.8.1.3.

5.7.3.3 TECHNICAL CAPABILITIES [C.2.10.8.1.4]

This section demonstrates the Level 3 Team's capabilities to meet the technical requirements for SMES listed in RFP Section C.2.10.8.1.4.

5.7.3.3.1 Monitor Email in Real-Time, on a 24x7 Basis, for Timely and Accurate Detection of Harmful Traffic and Unwanted Content

All of the Level 3 Managed Security Services are available to Networx customers 24x7. [redacted]

Section 5.7.3.3.2 below provides specifics of how we block harmful traffic and unwanted content.

5.7.3.3.2 Support Anti-Virus Scanning that Monitors all Inbound and Outbound Messages and Attachments

The Level 3 SMES offers the most complete protection in the world from email borne viruses and malware.

Our service will support Anti-Virus Scanning through a combination of techniques that will stop all known and unknown malware and virus threats from reaching a customer's network.

To identify and stop the back-catalog of known viruses, our solution [redacted] This technology will identify techniques

or characteristics that are indicative of an email virus – even if the virus is completely original in construction – thereby protecting customers from zero-hour outbreak attacks.

The Anti-Virus technology uses in identification include:

[redacted]

Acting as both a first, and last, line of defense, Level 3 offers both inbound and outbound protection, adding a much-needed additional layer of protection for the customer's network.

[redacted]

5.7.3.3.3 Support Anti-Spam Filtering that Prevents Unsolicited Marketing and Messages from Entering the Agency's Network, and Taxing Human, Bandwidth and Storage Resources.

The Anti-Spam Service is comprised of industry techniques, customer preferences and proprietary technology for identifying and stopping

unsolicited bulk email. A description of the anti-spam component or our SMES solution is described below.

[redacted]

[redacted]

- **Append a Header and Redirect to Bulk Mail Address** – This option will allow an agency to divert all identified spam to an email address held within the agency's infrastructure to allow a customer to control the spam emails.
    - This option is beneficial for customers who would like control of their identified spam. It allows an administrator to control which emails are released to the end users. This can be a large administrative overhead to organizations with large numbers of users.

[redacted]

The benefit of using "Append a Header but Allow Mail Through" is that the administration is passed to the end user and the identified spam will be separated from the legitimate emails. The end user can then look through the identified spam in the separate folder if they have a false positive.

[redacted]

- Agencies may choose to use this option if they would like to take away any overhead of dealing with spam. The downside of using this method is that legitimate emails (false positives) could be deleted.

[redacted]

[redacted]

5.7.3.3.4 Support Content Control, which screens inbound and outbound email for content that may signal system abuse or violation of agency communications policies

[redacted]

Content control is essential to meeting compliance with the growing regulatory environment surrounding electronic communications. Recent regulations, including laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Act of 2003 (SOX Act), explicitly mention civil and criminal penalties for security and data protection breaches.

In addition to compliance, agencies are facing other email security issues including threats to their employees, partners and customers. In an increasingly litigious world, it is essential that agencies protect themselves and their employees from internal and external email content threats by using the best solutions available. These threats include breach of confidentiality, loss of intellectual property, harassment of employees, defamation and obscenity, contractual liability, damage to business reputation not to mention wasted time and resources.

[redacted]

Deployed across our dynamic global platform, our SMES proactively [redacted] which will help agencies keep email clean and maintain agency integrity.

[redacted]

[redacted]

5.7.3.3.5 Respond to email infections and agency policy violations

[redacted]Notifications will not be sent to senders when the virus detected is a known spoofing virus. We will not send notifications when a false “from address” is used to prevent a false alarm to the "forged" sender. Notifications will also be sent to the administrators at the client.

Viruses are quarantined in advance of the network. [redacted] This allows us to quarantined viruses prior to reaching the agency's network. [redacted]

5.7.3.3.6 Support a secure web-based management interface

[redacted]

5.7.3.3.7 Queue and Retain Email in the Event of an Agency Mail Server or Connection Failure, in Order to Prevent Messages from Bouncing, and Gradually Transmit Queued Email upon Resolution of the Problem to Avoid Overloading the Servers.

The Level 3 SMES solution will queue mail for [redacted] in the event of a server failure at the customer site. Once the problem has been resolved, the service will allow for the gradual transmission of queued emails.

5.7.1.3.8 Implement Security Procedures to Preserve the Confidentiality and Integrity of All Agency Email Traversing its Network and Data Center

The privacy of agency emails will be paramount, and our security efforts will ensure that email passing through infrastructure is more secure than at any other stage in its travel across the Internet medium. Measures to maintain this privacy will include:

[redacted]

[redacted]

5.7.3.3.9 Support Email Requirements of Varying Complexity, in Terms of Load and Volume

The Level 3 SMES offering will accommodate a wide range of agency demands in terms of [redacted]

5.7.3.4 FEATURES [C.2.10.8.2]

RFP Section C.2.10.8.2 specifies no features for SMES.

5.7.3.5 INTERFACES [C.2.10.8.3]

In compliance with RFP Section C.2.10.8.3, Level 3's SMES will support the User-to-Network Interfaces (UNIs) defined in RFP Section C.2.4.1 Internet Protocol Service (IPS), as applicable.

5.7.4 Performance Metrics [C.2.10.8.4.1]

In accordance with RFP Section C.2.10.8.4.1, Level 3 will provide the performance metrics shown in Table 5.7-1 for our SMES offering. We note that SMES is a service that does not include the use of customer premise equipment, so there will not be an instance where a dispatch is necessary.

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

[redacted]

5.7.5 Proposed Performance Metrics

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.

5.7.6 Experience Delivering SMES

[redacted] Details are provided in Section 5.1.3.4 of this proposal volume.

5.7.7 Monitoring and Measuring KPIs and AQLs

The Level 3 Network Operations Center will monitor all (3)Enterprise services 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.

5.7.8 Optional Service Impact on Network Architecture

The SMES proposed by Level 3 will have little impact to a customer's network architecture. [redacted]

No additional network configuration will be required for this service.

5.7.9 NS/EP Functional Requirements

Section 2.5 of this proposal volume addresses how NS/EP requirements will be met for [redacted] services.

5.7.10 National Capital Region Service

Section 2.5.4 of this proposal volume discusses this topic in detail for all of Level 3's proposed services.

5.7.11 Meeting Section 508 Provisions

Reports generated as a result of an SMES engagement will be posted on the [redacted] portal. This 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 SMES 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.

5.7.12 Approach to SMES Technological Enhancements or Improvements

Level 3 fully expects that there will be many upgrades to the software and improvements to the service in the coming years. The SMES service is set up to make upgrading a simple procedure.

Prior to upgrading any component of the SMES service, the managed services team will fully test the upgrades to determine what impact, if any, the upgrade or change will have to the SMES environment. Once we determine the upgrade will not cause any negative impact on our SMES customer, we will roll out the update or improvement as part of the SMES offering.

There is always the chance that new technological enhancements and improvements will cause compatibility issues with the SMES service. If this is the case, our Managed Security Services engineering team will work to overcome any compatibility issues and roll out new technology and capabilities to ensure the SMES is competitive in the marketplace.