

VOLUME 1, SECTION 5.4: ANTI-VIRUS MANAGEMENT SERVICE



5.4 ANTI-VIRUS MANAGEMENT SERVICE [C.2.10.4, M.2.1.3]

The Level 3 Team’s Anti-Virus Management Service (AVMS) will meet or exceed the Government’s requirements for AVMS, as defined in RFP Section C.2.10.4. This section provides a description of this service offering followed by responses to the specific requirements listed in RFP Section L.34.1.6.

The Level 3 AVMS solution will provide [REDACTED] virus protection for in-bound and out-bound email, file transfers and web traffic. The solution, illustrated in [REDACTED] will also allow for [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

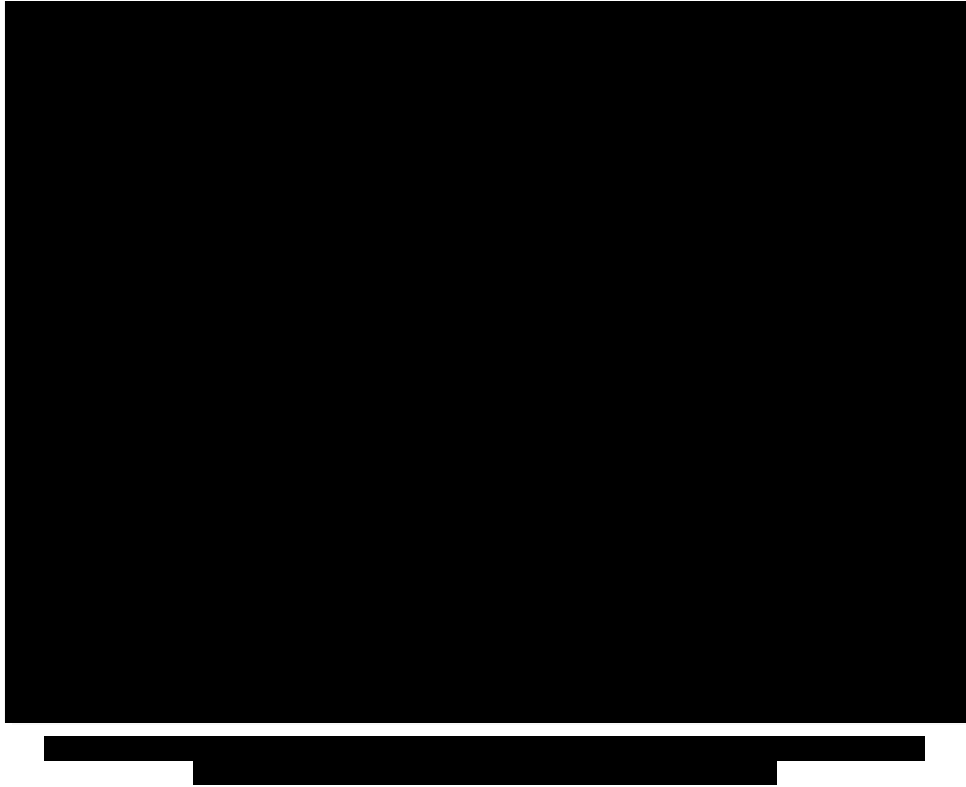
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


Level 3 will continually monitor anti-virus advisories for complete understanding of the ever-changing virus landscape. Agencies will be able to leverage our [REDACTED] security staff to protect their networks from virus threats, freeing up your security staff to focus on security management.



5.4.1 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 Anti-Virus Management Service. The topics covered include our approach to Service Delivery, our approach regarding Federal agency Enterprise Architecture objectives, and any foreseen problems and solutions related to our offering.

5.4.1.1 SERVICE DELIVERY

The Level 3 Service Delivery objective is to provide Government agency customers with rapid and responsive Service Delivery for our Anti-Virus Management Service. All services proposed by the Level 3 Team for  will use the same Service Delivery process. Level 3’s

Network delivery process is discussed in detail in Section 3.1.1.1 of this proposal volume.

5.4.1.2 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.

5.4.1.3 FORESEEN PROBLEMS AND SOLUTIONS

The Level 3 Team has reviewed the individual service requirements for AVMS in RFP Section C.2.10.4.1. We do not anticipate any problems meeting the specified service requirements. In the unlikely event that a problem does arise, our security engineering team will work with the agency to customize a solution to meet the requirement.

5.4.2 Satisfaction of Security Services Performance Requirements [C.2.10.4.4]

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.

5.4.2.1 QUALITY OF SERVICE

In compliance with RFP Section C.2.10.4.4, Level 3 will provide the performance metrics shown in [REDACTED].

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

5.4.2.2 MONITORING AND MEASURING KPIs AND AQLs

The Level 3 [REDACTED] will monitor all Network 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 AVMS are described below.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

5.4.2.2.2 Time to Restore

Unlike many service providers, Level 3 measures the Time to Restore (TTR) as the customer-facing time to restore a problem. Our metric represents the gross internal performance of our service management teams. Specifically, the duration of an unexcused outage on an AVMS port would be measured from the time a trouble ticket is opened to the time that service is restored.

5.4.2.3 TESTING PROCEDURES FOR KPI AND AQL

Section 2.2.3 of this proposal volume provides a discussion of the management expertise and toolsets used by Level 3 to ensure KPI and AQL compliance.

5.4.2.4 PROPOSED PERFORMANCE IMPROVEMENTS

Level 3 does not propose AQLs that 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, available services.

5.4.2.5 PROPOSED PERFORMANCE METRICS

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

5.4.3 Satisfaction of Security Services Specifications

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

5.4.3.1 TECHNICAL DESCRIPTION OF AVMS

The Level 3 Anti-Virus Management Service offering fulfills the Mandatory Service Requirements for AVMS contained in RFP Section C.2.10.4.1. This section demonstrates our capabilities in the following areas:

- Standards
- Connectivity
- Technical Capabilities
- Features
- Interfaces

5.4.3.1.1 Standards [C.2.10.4.1.2]

The Level 3 AVMS complies with the required standards as delineated in RFP Section C.2.10.4.1.2. 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)

5.4.3.1.2 Connectivity [C.2.10.4.1.3]

Level 3 is a Tier 1 Internet Service Provider. Our AVMS offering meets the connectivity requirements listed RFP Section C.2.10.4.1.3.

5.4.3.1.3 Technical Capabilities [C.2.10.4.1.4]

Our AVMS solution complies with the 15 mandatory technical capabilities requirements listed in RFP Section C.2.10.4.1.4. Details follow.

1. Provide design and implementation services:

The Level 3 Team has a five-phase approach to design and implementation services, which is standard for our Managed Security Services. Please see the response to Section 5.3.3.1 3 for details.

2. Provide installation, configuration and integration support:

[REDACTED]

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. All Level 3 service and design features deployed in the network may be replicated using every type of element in the actual production network. Replication of real-network element behavior under realistic traffic load conditions is critical to producing accurate test results.

Regression and performance testing is completed on all features of the Level 3 Network. This includes [REDACTED] [REDACTED] New procedures and tools, such as new network management and provisioning tools, are tested before deployment. Even maintenance procedures are tested before they are performed on the network.

Many service providers use their in-band Internet backbone as their primary management network. Some have an out-of-band (OOB) network,

usually dial-up, or very low bandwidth switched data services such as Frame Relay. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

3. Provide software and hardware components, including servers and gateways, as required by the agency:

Level 3 will provide the necessary hardware and software. The AVMS offering includes [REDACTED]

4. [REDACTED] System Monitoring:

The Level 3 [REDACTED] will be responsible for all facilities and network management, monitoring, and repair associated with the proposed managed tiered security services. The Level 3 Network group is staffed by highly trained operations managers and network technicians at [REDACTED]
[REDACTED]

The [REDACTED] provides proactive monitoring of customer traffic across the Level 3 Network. It identifies potential problems and provides resolution before our customers even know there's an issue. The [REDACTED] performs regular network connectivity performance reviews. If an irregularity is detected, the organization follows documented procedures to restore service.

The Level 3 Team's concept of operations integrates network surveillance performed by the [REDACTED] to provide seamless coverage and end-to-end management of all critical



network elements. The [redacted] will serve as liaison between the Level 3 [redacted] and the [redacted]. The [redacted] staff will gather performance data on the systems supported and use these data to optimize network efficiency and help Government agencies avoid unnecessary costs.

Level 3 will monitor the AVMS engines [redacted]
[redacted]
[redacted]

5. Allow real-time and on-demand virus scanning:

The Level 3 AVMS offering includes the ability to do real-time as well as on-demand virus scanning.

6. Screen incoming and outgoing FTP, HTTP, POP, and SMTP traffic:

The Level 3 AVMS offering provides [redacted] virus protection for in-bound and out-bound email, file transfers and web traffic.

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

7. Perform data integrity checks:



The Level 3 AVMS offering is based on [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- 8. Respond to infections and violations of agency networking environment and provide the following minimum capabilities: Alert Service, Infected File Isolation and Control of user access and environment for the malicious file:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

9. Maintain the anti-virus system and perform the necessary hardware/software upgrades, updates, and replacements:

As part of the AVMS offering, Level 3 will maintain the [REDACTED] anti-virus platform and software and provide all the necessary hardware/software upgrades and updates. All hardware replacements will be handled on the agency's behalf through the vendor's support contracts.

10. Deploy the latest system patches and bug fixes as soon as they become available:

As part of the AVMS offering, Level 3 will be fully responsible for all system patches and bug fixes. All updates other than virus pattern updates must be certified by Level 3 personnel prior to being released to production. These updates include, but are not limited to:

[REDACTED]

11. Provide automatic and timely updates of the virus pattern and signature files as they become available to ensure adequate protection:

[REDACTED]

12. Perform periodic gateway scans capable of revealing any vulnerabilities of the anti-virus system:

The Level 3 Team will provide scans of the [REDACTED] deployment. The vulnerability scans will determine what vulnerabilities, if any, are present on the AVMS platform.

As part of the managed AVMS offering, Level 3 will take full responsibility for patching and updating the AVMS platform. This will ensure all applicable security patches are placed on the platform in a timely manner, lessening the chance of vulnerabilities existing on the AVMS platform.

13. Perform configuration changes as initiated and prioritized by the agency:

The Level 3 Team’s AVMS includes unlimited changes to the AVMS device. As a fully managed solution, we will be responsible for making all the changes to the AVMS hardware and software.

On average, Level 3 completes more than [REDACTED]

Our process provides the rigor and discipline necessary to minimize the risk of change while at the same time providing flexibility and adaptability to allow our customers to meet their critical requirements.

The Level 3 Configuration Management procedure is described below. Note that our procedures ensure that no changes initiated by our team will be implemented without agency consent.

14. Change Management Process:

A detailed discussion of Level 3's Change Management Process is provided in Section 5.2.3.1.3.16 of this proposal volume.

15. Provide agency with secure web access to logs and service information:

The Level 3 [redacted] portal will provide the agency with online access to logs and service information, which will contain, but not be limited to, the following, as applicable:

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

As noted previously, the [redacted] portal will provide agencies with insight into the performance of Level 3 services. [redacted]

[redacted]

[redacted] The portal gives direct access to the monitoring and maintenance systems used by Level 3 internal staff.

Agencies can use the [redacted] portal to report and/or obtain status information for ongoing events. The portal will provide the ability to view all current issues, provide updates to ongoing issues, open trouble tickets, and allow escalation of individual tickets or issues. It will also provide the agency

with immediate access to severe alert information including: [REDACTED]

[REDACTED]

16. Support networks of varying complexity:

[REDACTED]

5.4.3.1.4 Features [C.2.10.4.2]

[REDACTED]

5.4.3.1.5 Interfaces [C.2.10.4.3]

[REDACTED]

5.4.3.2 PROPOSED SERVICE ENHANCEMENTS

The Level 3 Team does not propose service enhancements to AVMS 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.

5.4.3.3 NETWORK MODIFICATIONS

We anticipate the need for very minimal modifications to the network for delivery of AVMS, with negligible impact on the security or performance of the network. These modifications are described below.

[REDACTED]



5.4.3.4 EXPERIENCE DELIVERING AVMS

The Level 3 Team leads the industry in planning and deploying Managed Security Services for both the commercial and Government sectors. We bring five years of experience delivering anti-virus services to customers worldwide.

Section 5.1.3.4 of this proposal volume further demonstrates our team's experience and credentials in the managed security arena.