VOLUME 1, SECTION 2.0:

NETWORX ARCHITECTURE FOR ENTERPRISE PROPOSAL FOR IP-BASED SERVICES

2.0 NETWORX ARCHITECTURE FOR ENTERPRISE PROPOSAL FOR IP-BASED SERVICES [M.2.1.1]

The Level 3 Enterprise Networx solution, (3)Enterprise[SM], for the GSA combines the world-class Level 3 Network and broad geographic coverage with our extensive experience gained through [redacted] years of providing robust, technologically advanced network services to major network providers and large enterprise customers.

In [redacted], Level 3 began building a next-generation global IP network from the ground up. [redacted] [redacted] later, we transitioned our first customers onto this converged IP network supporting data, voice, video, and wireless on a single end-to-end network.

Industry recognition of the Level 3 ability to execute and deliver a technically superior solution and a proven operational and support model includes awards such as the Frost & Sullivan “Next-Generation Service Provider of the Year” award and the Computerworld “Smithsonian Laureate” award for leadership in the information revolution. These two examples point to the Level 3 ability to help our customers achieve their goals, and our commitment to managing their networks, enabling them to focus on their core missions.

The Level 3 Network is a [redacted] IP-based network, and thus is more adaptable to future technological changes than existing, less-flexible networks. No other provider can match Level 3’s ability to expand capacity or adopt new technology and services while limiting operational inefficiencies.

This section of the proposal addresses the requirements from Section L.34.1.3 of the RFP. The Level 3 Team has developed an extensive portfolio

of services for agency telecom and networking requirements to be delivered using commercially available Level 3 Team products or services. This provides the GSA a low-risk communication solution for Government agency customers built on access to fully-mature, well-tested, commercial services.

Section 2.1 describes our approach to meeting the information security needs of Government agencies. Our infrastructure provides protection against cyber attacks in addition to planning for physical security and other regulatory-driven security requirements.

Since our founding, Level 3 has strived to create a facts-based process management culture. Our [redacted] methodology is an ongoing effort to measure results, analyze root causes of problem areas, institute irreversible corrective actions and service improvement, and control the process through frequent reviews. We believe these methods drive our customer focus and the pursuit of excellence—the same methods we will use to ensure our (3)Enterprise services are both highly reliable and meet the GSA quality requirements. Our approach to ensure quality and reliability is described in Section 2.2.

The Level 3 Team is committed to providing the Government with Networx services based on proven, mature technology that offers the best performance possible for convergence and interoperability. We constantly review opportunities to upgrade our services as technology advances, after the changes have been fully tested and shown to meet the needs and expectations of our customers. Our approach to convergence, interoperability, and evolution is discussed in Section 2.3.

Section 2.5 describes the Level 3 ability to provide service to Government customers during emergencies, such as national security and natural disaster events. Protection of our signaling systems and assurance of coverage in

our National Capital Regions is discussed. Section 2.5 also covers our compliance with the provisions of Section 508.

VOLUME 1, SECTION 2.1:

APPROACH TO ENSURE INFRASTRUCTURE SECURITY

2.1 APPROACH TO ENSURE INFRASTRUCTURE SECURITY [M.2.1.1 (B)]

Infrastructure security assurance will be accomplished through compliance with [redacted] Federal Information Processing Standard (FIPS) and the National Institute of Standards and Technology (NIST), as required for the Government's compliance with the Federal Information Security Management Act (FISMA). Sub-contractors will function under the Level 3 Federal Security Management (FSM) Program in a [redacted] manner. [redacted]

The guiding security principles contained in NIST Spec Pub 800-14, NIST Spec Pub 800-64 and the security engineering principles defined in NIST Spec Pub 800-36 will be used [redacted] Related non-security FIPS and NIST Spec Pubs will be used [redacted]

The selection, implementation, and management of security related, or enabled, products will be based on the [redacted]

[redacted]

One of the guiding principles at Level 3 is the concept of [redacted] or [redacted] security using discrete platforms and processes. There are always at least [redacted] levels of security that must be traversed to access any particular resource in the (3)Enterprise Operation Support Systems (OSS).

GSA has indicated a FIPS 199 Impact Low system as part of the Risk Assessment (RA) required by statute during the initiation phase. This system of categorization indicates that the GSA has determined that the security objectives of [redacted], [redacted] and [redacted] for all data elements under the contract are [redacted], as defined [redacted] Since the RFP doesn't specify FISMA/FIPS-compliant control enhancements, the Level 3 Team will use [redacted]

2.1.1 Infrastructure Protection and Service Security

The FISMA-compliant OSS infrastructure components, including personnel, used for the (3)Enterprise will be segregated, [redacted] from our commercial OSS. The (3)Enterprise-related infrastructure will be FISMA/FIPS-compliant and use all the mandatory requirements specified by FISMA, FIPS 199, FIPS 200 and related reference publications and documents specified therein for a FIPS 199 Low Impact system. A Low Impact system is determined and specified by the GSA under their non-assignable statutory requirement to categorize the FIPS 199 System Impact Level during the initiation phase of the project. These infrastructure

components are under the control and supervision of our FSMP and the client agency Security Management Program as required by statute.

Level 3 will use [redacted] compliant SmartCards for access [redacted]

At Level 3, the (3)Enterprise OSS environment is comprised of [redacted] systems and [redacted] applications, as identified in the [redacted]. [redacted]

The network [redacted] and [redacted] resources within these system boundaries are configured with [redacted] All [redacted] resources within the system boundaries are managed using [redacted] conforming to the requirements [redacted]

User and operator access to the (3)Enterprise OSS is performed [redacted]

[redacted]

Any security-related events associated with the referenced systems will be handled by staff in the [redacted] that [redacted] and [redacted] the [redacted]

[redacted]

[redacted] resources are configured with guidance from [redacted] as applicable.

[redacted] user access to server resources is performed [redacted]

[redacted]

Communications between [redacted] resources within [redacted]

[redacted]

[redacted]

2.1.2 Protection Against Cyber Attacks

While Section 2.1.1 deals with the FISMA compliant [redacted] requirements, Section 2.1.2 describes the security functions related to Level 3 commercial infrastructure supporting the (3)Enterprise OSS. Transitions between the commercial infrastructure and (3)Enterprise OSS infrastructure are noted where applicable. For each commercial infrastructure function or resource listed, there is a corresponding FISMA-compliant (3)Enterprise OSS function or resource.

Level 3 is very aware of the increasing incidence of cyber attacks occurring in the Internet. We understand the impacts that these attacks could have on Government agencies and our commercial customers. We rigorously defend our network infrastructure by employing a wide variety of methods, procedures, and systems. In this section, we describe the measures taken to protect our network from various types of cyber attacks.

2.1.2.1 FISMA COMPLIANT (3)ENTERPISE OSS COMPONENTS AND SYSTEMS

The Level 3 FISMA-compliant (3)Enterprise OSS components and systems will be [redacted] segregated from Level 3 non-FISMA-compliant commercial services and operational support systems. In effect, the (3)Enterprise OSS is [redacted] within, and [redacted] by, our commercial infrastructure. This [redacted] provides protection for the (3)Enterprise OSS from [redacted]

2.1.2.2 ISP SECURITY CONSORTIUM

Level 3 is a charter member of the Internet Service Provider (ISP) Security Consortium. Level 3 has pledged to work with other ISPs on specific detection, prevention, and tracing options that can be deployed industry-wide.

2.1.2.3 LEVEL 3 NETWORK SECURITY OPERATIONS

The Level 3 [redacted] Team protects provided services and the associated commercial and (3)Enterprise OSS infrastructure. The [redacted] team protects against network threats and malicious or unauthorized network access. Several types of threats that concern[redacted] include the following and more:

[redacted]

The Level 3 [redacted] team is divided into [redacted] main groups[redacted] Each group is responsible for specific [redacted] issues. The types of security issues, or event categories, each group manages, are as follows:

[redacted]

Level 3 [redacted] manage a variety of event types in an effort to insure the integrity of The Level 3 Network. Events directly associated with, or impacting, the (3)Enterprise OSS infrastructure will be handled by staff specifically cleared and trained for the (3)Enterprise Program. [redacted]

[redacted]

[redacted]

Events are categorized as one of the following types:

[redacted]

When an alarm is received, the [redacted] performs the following tasks:

[redacted]

2.1.2.4 Out-of-Band Management Network

Level 3 maintains a unique high speed, diverse, [redacted] management network for all its [redacted] devices. This allows us to have a significant additional layer of security for network devices by restricting management access to the [redacted] network only. In addition, the [redacted] network

allows greater flexibility in accessing network elements during maintenance events and outages.

The Level 3 Network provides the following security-related features:

[redacted]

2.1.2.5 NETWORK VULNERABILITY ASSESSMENT

Every single network element is scanned at [redacted] a day for vulnerability issues. Level 3 uses the following [redacted] to check for vulnerability exposures:

[redacted]

Inventory Tool: Polls the network to identify new systems and profile changes to existing systems

If a vulnerability issue is identified, the [redacted] team takes the following actions:

[redacted]

2.1.2.6 MITIGATING DOS ATTACKS

DOS attacks can impact the integrity of a network and directly impact its service performance. They can also impact the service performance of multiple networks [redacted]

Level 3 employs [redacted] different methodologies for mitigating DoS attacks. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

2.1.3 Best Practices

[redacted]

Since the passage of FISMA, the definition of "best practices" is defined by statute as the FIPS and is related in NIST Spec Pubs when discussing Executive Federal Information Systems covered under FISMA. Private sector industry standards can be applied when they meet the FISMA/FIPS minimum requirements but still must be applied within the FISMA/FIPS framework.

In the case of the FISMA-compliant (3)Enterprise OSS and related FISMA-compliant infrastructure, the definition of best practices follows the guiding principles as defined in the [redacted]. The particular [redacted] covering the baseline principles used to define "best practices" for the FISMA compliant (3)Enterprise infrastructure are listed below:

[redacted]

These [redacted] provide the basis for "best practices" for FISMA-compliant systems through all phases [redacted] either directly or through reference. [redacted] The validation for successful implementation of "best practices" for FISMA-compliant systems is the NIST Certification and Accreditation (C&A) process as discussed in Section 2.1.5 of this proposal volume.

[redacted]

2.1.4 Infrastructure Security Enhancements

When considering implementation of security enhancements, the set of standards applicable to the system or service needs to be considered. There are stringent regulatory requirements for FISMA-compliant systems.

Under FISMA, there is an intentional disconnect between commercial offerings and Government offerings when there is a FISMA compliance requirement for the services and/or systems used by the Government.

[redacted]

First and foremost, there must be a FISMA, FIPS, and/or NIST-related reason for upgrading the security of a system that is already certified and accredited. Basically we foresee [redacted] instances where changes to the security infrastructure of the (3)Enterprise OSS and infrastructure will be necessary:

[redacted]

[redacted]

2.1.5 Certification and Accreditation

The Level 3 Team, including our subcontractors, have staff with broad experience in developing C&A packages for numerous Federal agencies for Executive Systems covered under FISMA and various other projects.

The Level 3 Team will derive primary C&A guidance from [redacted]

[redacted]

The Level 3 process specifically includes developing documents in accordance with guidance contained in [redacted] and will include the following:

[redacted]

Level 3 will provide this documentation to the responsible Government entity [redacted] working days ahead of the C&A due date (excluding the period of December 1 to January 5 unless explicitly requested). In accordance with [redacted], Level 3 will assign personnel to execute the following roles [redacted]

[redacted]

[redacted]

A subset of such personnel may be preferable, but this is up to the discretion of the working committees. The C&A process can either follow [redacted]

The overall goal of C&A is to protect Governmental Information Systems from both [redacted] and [redacted] network intrusion or attempts at system security compromise. [redacted]

The Level 3 C&A team will meet with the corresponding Government representatives [redacted]. [redacted]

The key to finalization [redacted] as follows:

[redacted]

Certification Phase: [redacted]

The Accreditation Phase: During this phase, Level 3 will work with the Government to achieve final accreditation and perform any final changes or improvements that may be necessary to complete the accreditation. [redacted]

[redacted]

Level 3 will insure that upon successful completion of C&A, the authorization to operate the information system will strictly follow Government-approved requirements. [redacted]

Continuous Monitoring Phase: Monitoring enforces everything that has been put together in the first three phases. [redacted]

[redacted]

[redacted] This is advantageous to both Government agency customers and Level 3, since streamlined processes can be defined and executed for such systems.

[redacted] tests and evaluations are a critical aspect of the C&A process, and primary guidance will be derived from [redacted] Testing verifies target system compliance with associated security requirements [redacted]

requirements). Once vulnerabilities have been identified, we will [redacted]