

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3.4 Step 4: Assess Security Controls [L.29.3.b), C.2.8.4.5]

The assessment plan has three phases:

- Phase 1: [REDACTED]
[REDACTED]
[REDACTED]
- Phase 2: [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- Phase 3: [REDACTED]
[REDACTED]
[REDACTED]

3.5 Step 5: Authorize Information System [REDACTED] [L.29.3.b), C.2.8.4.5]

Once our internal assessment activities are completed, Level 3 will seek to authorize the system through GSA.

3.6 Step 6: Monitor Security Controls [L.29.3.b), C.2.8.4.5]

As noted above in Section 3.2.3, we expect to automate the monitoring process to a practical level as only automation can provide near real-time monitoring.

3.7 Schedule [L.29.3.b), C.2.8.4.5]

Figure 3.7-1 is Level 3's the current schedule for its development of [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]	[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]	[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]
[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]	[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]	[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]	[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]	[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]	[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]
[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]	[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]	[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]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

3.8 [REDACTED]

[REDACTED]

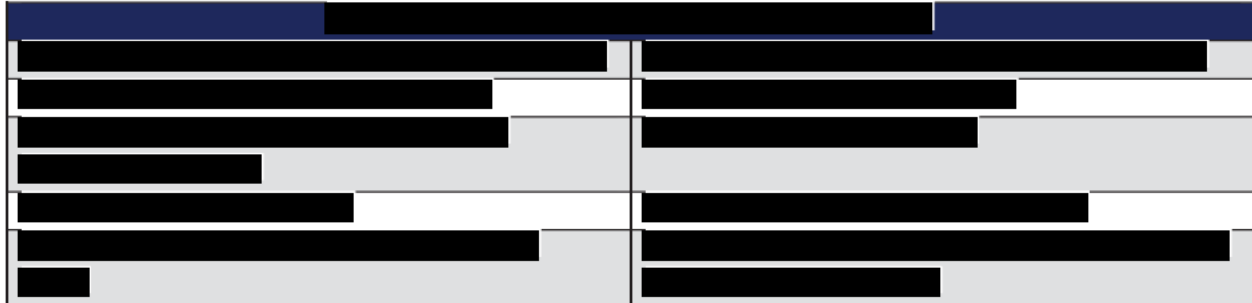
[REDACTED] a supply chain risk management methodology, described in this section, which is designed to meet the Government's requirements for the EIS

[REDACTED]
using National Institute for Science and Technology (NIST) Special Publications 800-161 and 800-53 Revision 4 (including SA-12). In addition, to using the Government's

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

NIST SCRM publications as a guide for the foundation to our [REDACTED], shown in Figure 3.8.1-1.

Figure 3.8.1-1. NIST's [REDACTED]



Level 3 is dedicated in supporting GSA's objective to ensure that an adversary will not sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to [REDACTED]. In addition, Level 3 is committed to addressing GSA's intent to mitigate the threat of counterfeit and illegally modified products, and the enforcement of strict quality control across the supply chain environment.

3.8.2 Organizational Support

This document outlines Level 3's policies, processes and controls and will be focused on meeting [REDACTED]

[REDACTED] Level 3 understands the importance of implementing risk management processes that address counterfeit and illegally modified products. Our risk management policies and processes will provide the framework for Level 3 personnel to mandate, support and enforce appropriate measures in the mitigation of supply chain vulnerabilities. The five supply chain phases include: [REDACTED]

[REDACTED] are key areas of focus included in the risk management plan set forth in the [REDACTED]

SCRM Plan annually and when significant changes occur.

3.8.2.1 Organizational Framework and Participation

Level 3's executive team is committed to ensuring that potential supply chain threats are closely monitored to minimize any negative impact to [REDACTED]. Our plan is to begin with a management strategy that is a three-step process built on a strong executive commitment to securing the Level 3 infrastructure as shown in **Figure 3.8.2.1-1**.

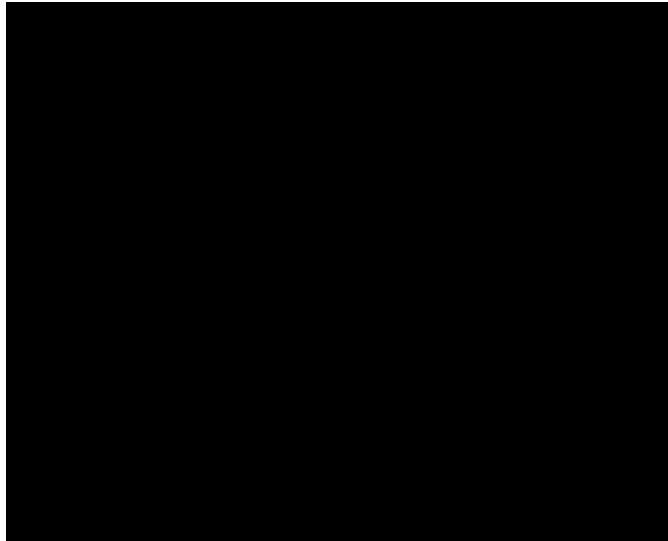


Figure 3.8.2.1-1. Risk Management Organizational Participation.

- **The Executive Team** establishes the appropriate structure and strategy for managing supply chain risk. The executive team has a keen understanding of the inherent risks involved in supplying EIS services. It is of critical importance to be vigilant as a service provider in identifying, managing, and mitigating supply chain risks to GSA for the EIS. The enforcement of strict quality control by Level 3 of the applicable [REDACTED] mission and vision statement, the executive team is focused on protecting the Level 3 EIS infrastructure and customer information from physical and logical threats by stating:

Executive Team Mission

“Our mission is to ensure the security integrity of Level 3’s EIS services from adversaries who look to sabotage Level 3 EIS service infrastructure and/or customer information through surveillance, denial or disruption of service either physically or logically.”

Executive Vision

“To protect the physical and logical security of the Level 3 EIS Services.”

- **The Business Processes** consist of the following tasks to be carried out by key functional areas within the Level 3 organization for the EIS [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED], to ensure the risk

management strategy is adhered to.

- **The Information Technology** involves the Level 3 [REDACTED] [REDACTED] security boundary. Numerous functional areas within Level 3 may be included in the review of supply chain management risk but are not limited to: Product Management, Contracts and Legal, Network Architecture and Development, Backbone Engineering, Global Procurement and Corporate Security.

3.8.2.2 Organizational Support Model [L.30.2.2 (1), G.6.3 (1)]

To ensure that supply chain risks are effectively assessed, managed, documented, tracked, and controlled, Level 3 recognizes that key stakeholders from various functional areas within the organization may be involved in overseeing supply

chain risk management. This group of stakeholders will make up the Level 3 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] shown in **Figure**

3.8.2.2-1. Level 3 recognizes the need for key functional areas to be engaged in ensuring risk levels are minimized and the integrity in the supply chain remains intact.

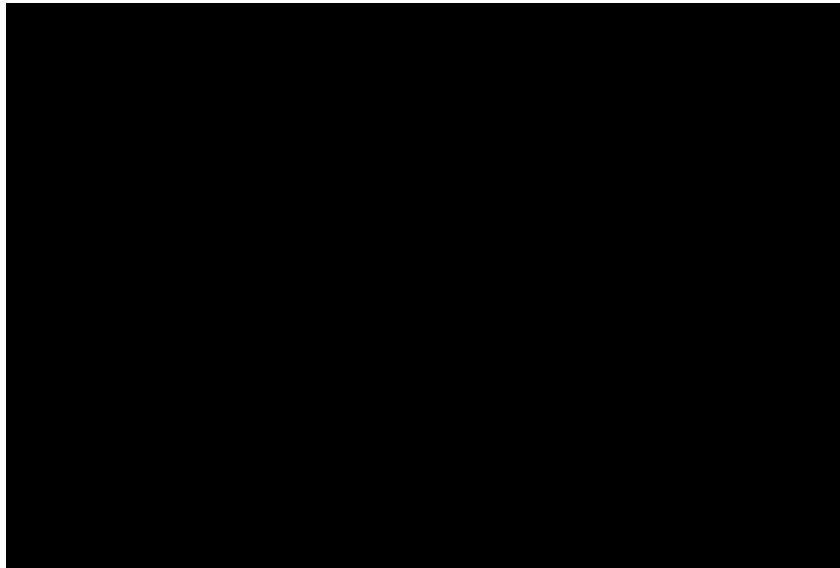


Figure 3.8.2.2-1. Level 3's SCRM Organizational Support Model.

3.8.2.2.1 Roles and Responsibilities

Procurement, Vendor Management, Corporate Security, Security Architecture Engineering Legal, Program Management Office (PMO), Network Operations, and Training. Other internal groups may also be involved during various milestones within the supply chain lifecycle.

Level 3 has created a preliminary responsibility assignment matrix [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] It is the expectation that additional controls and tasks will be added as risks are assessed and examined.

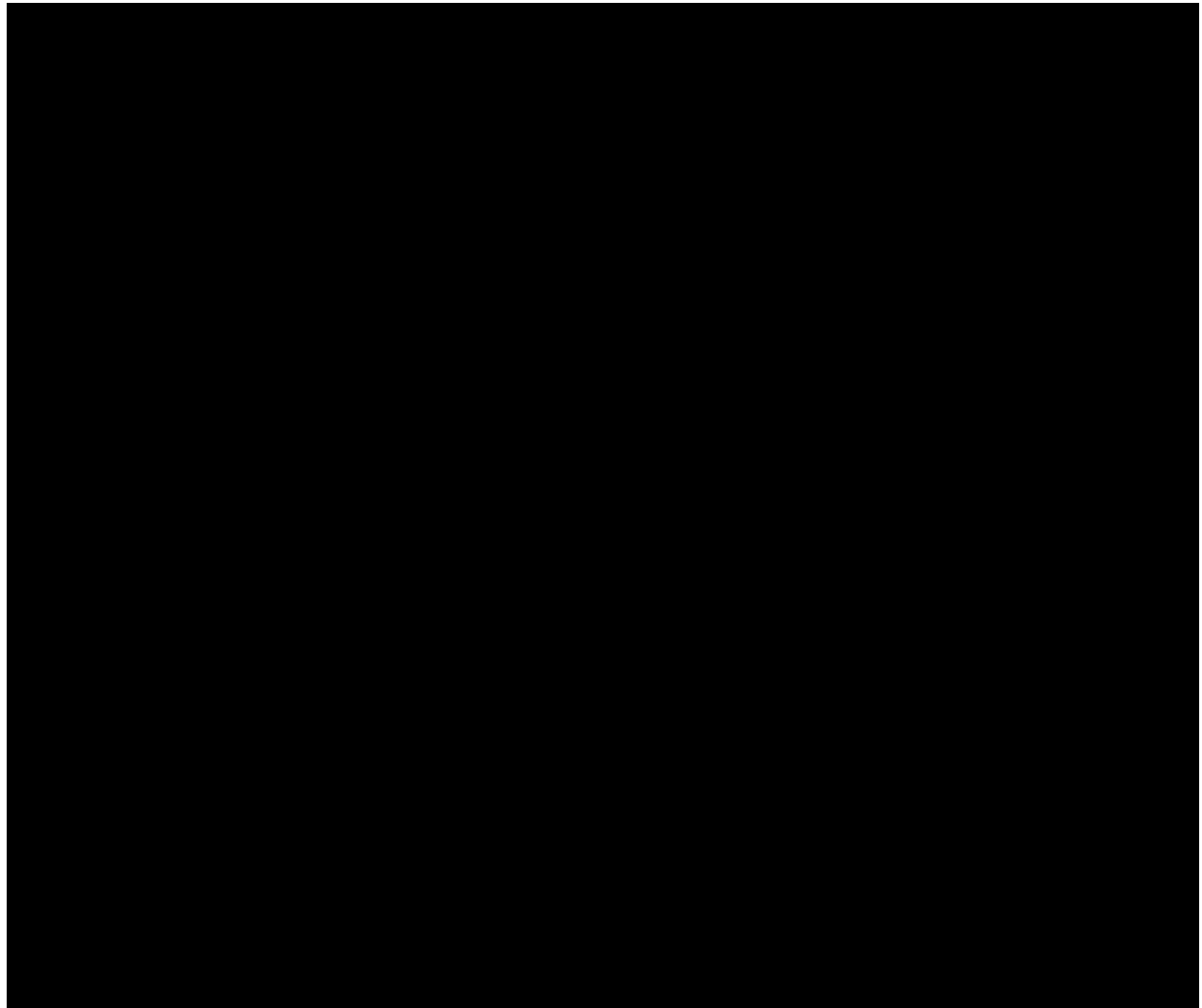


Figure 3.8.2.2.1-1. Preliminary [REDACTED] Framework.

The [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] is nimble enough to not only support GSA's over-arching contract vehicle, but be able to be tailored to the unique characteristics of each task order. Level 3 recognizes that both the controls and

areas of responsibility may vary on a task-order to task-order basis. Therefore, Level 3 acknowledges that there will need to be a rigorous, yet flexible approach to the implementation of the [REDACTED] over the life of the IDIQ contract.

3.8.2.2.2 Supply Chain Risk Management Approach

Level 3's strategy for supply chain risk management will be proactive in identifying risks that could impact the integrity of the applicable services. The [REDACTED] will outline the required mitigation steps necessary to proactively mitigate or control risks. Level 3's goal is to mitigate the possibility of disruptions or degradations to the applicable EIS services. **Figure 3.8.2.2.2-1** shows the [REDACTED] process for managing risks and threats to the applicable services.

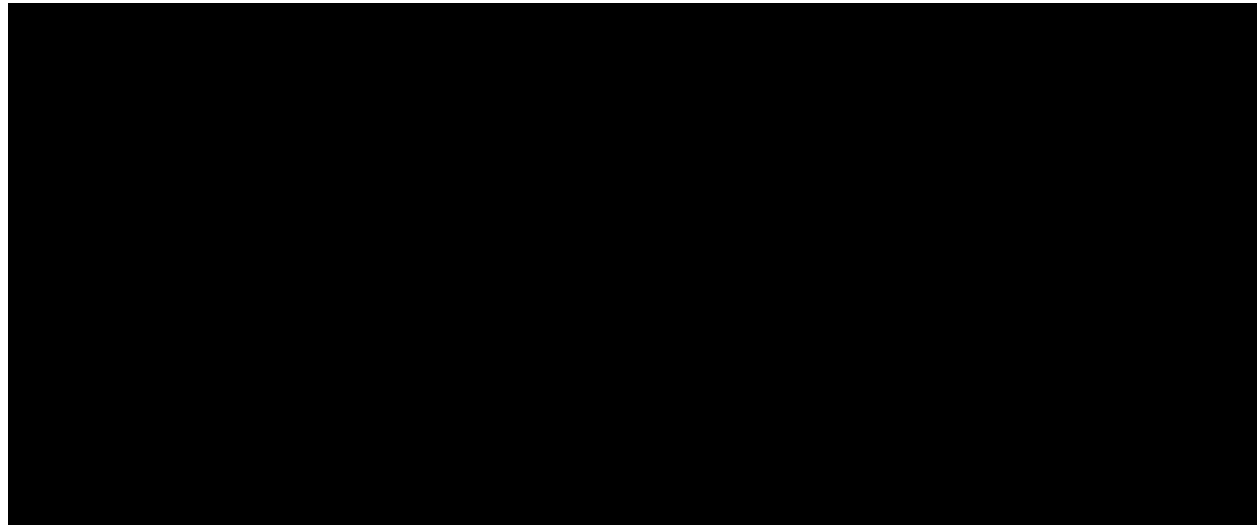


Figure 3.8.2.2.2-1. Level 3's [REDACTED] Approach.

Supply chain risk information will be reviewed periodically. Each identified risk [REDACTED] [REDACTED] [REDACTED] [REDACTED] will be executed immediately to contain risk and safeguard areas of vulnerability.

3.8.2.2.3 Supply Chain Risk Management Processes

Supply chain risk management is an organized methodology for continuously identifying and measuring the issues that may impact applicable services. The process involves developing mitigation steps; selecting, planning, and implementing appropriate risk mitigation strategies or solutions; tracking and documenting risk to ensure successful risk reduction/mitigation acceptance. Effective supply chain risk management depends on planning early identification and analyses of risks associated with software, hardware and professional services. In addition early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, training, coordination and organizational collaboration are keys to a successful SCRM Plan implementation.

Before approving a supplier who may be providing professional services, software or hardware related to the [REDACTED] multiple Level 3 organizations will become engaged in managing risks associated with supply chain lifecycle. To effectively manage risks, Level 3's [REDACTED] [REDACTED] (Figure 3.8.2.2.3-1). Suppliers are monitored for risks during the lifecycle of their contract and/or warranty period to mitigate any potential risks.

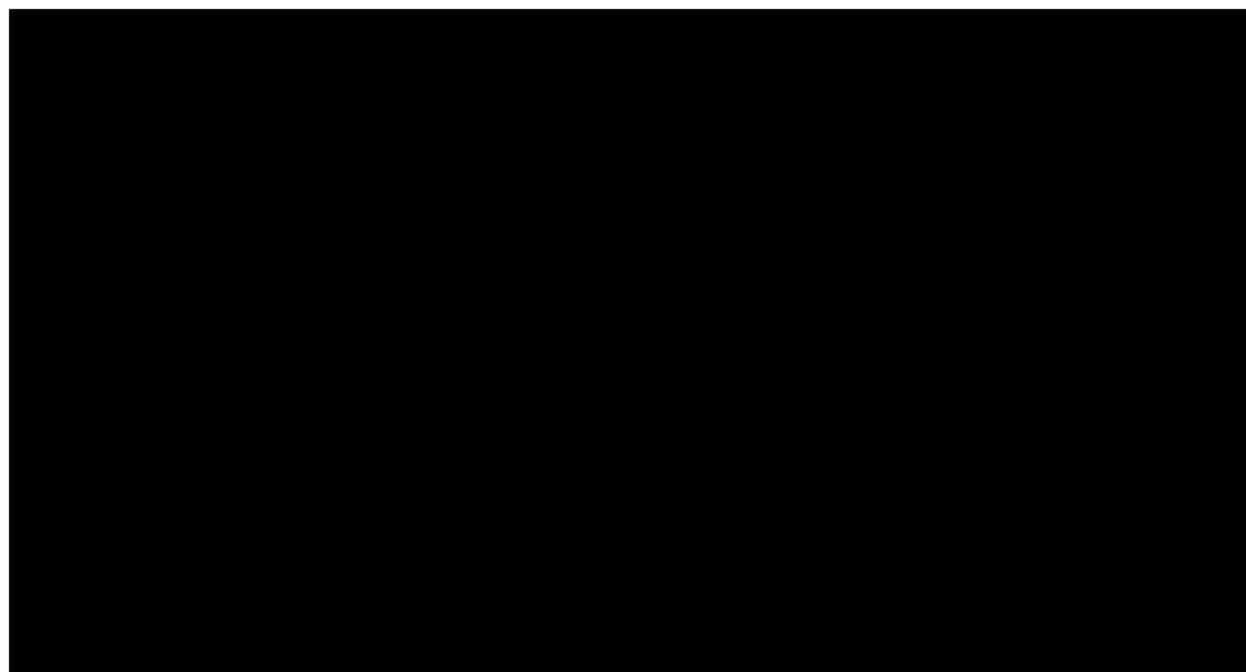


Figure 3.8.2.2.3-1. Level 3's

Process.

3.8.2.2.4 Supply Chain Risk Notification and Analysis

Level 3's supply chain risk identification and risk analysis is the responsibility of various technology and operational groups within Level 3. These groups work in teams and have the responsibility for gathering transport statistics and data to help facilitate supply chain risk analysis. Once the analytical work is carried out and areas of vulnerabilities are identified, specialized organizational teams will administer mitigating controls to the [REDACTED] utilizing the assignment of user accounts and passwords and other security controls.

Figure 3.8.2.2.4-1 shows the process for communicating risks to internal teams within the Level 3 organization. If a risk is identified as a 'critical' risk, our internal teams will schedule an emergency meeting to address and mitigate the risk.

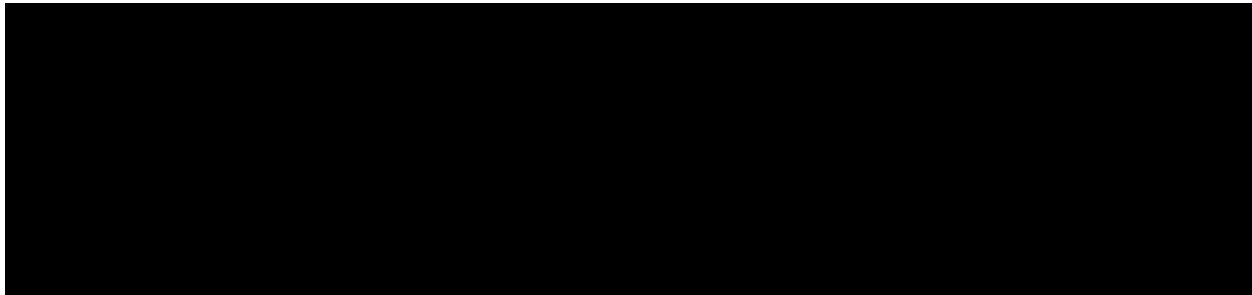


Figure 3.8.2.2.4-1. [REDACTED] **Process.**

3.8.2.2.5 Policy Directives and Guidelines Followed

Supply chain risk management and analysis activities for the [REDACTED] use the following guidelines as a reference as deemed appropriate:

- NIST 800-161, June 2014, **Supply Chain Risk Management Practices for Federal Information Systems and Organizations**
- NIST SP 800-30, September 2012 - Risk Management Guide for Information Technology Systems
- NIST SP 800-53 Revision 4, April 2013 and Latest Publication - Security and Privacy Controls for Federal Information Systems and Organizations (i.e., SA-12 controls)
- Federal Information Processing Standards (FIPS) Publication 199/200, February 2004 and March 2006

- DoD Instruction 5200.39, July 2008 - Critical Program Information (CPI) Protection within the Department of Defense
- DoD Instruction 5200.44, November 2012 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- National Institute of Standards and Technology Internal Reports (NISTIR) 7622, October 2012 - Notional Supply Chain Risk Management Practices for Federal Information Systems

3.8.2.2.6 Supply Chain Risk Management Plan Change Control

Level 3 has defined a process for updating the [REDACTED]

[REDACTED] The internal functional teams will work collectively to identify new or modified controls and authorize updates to the master [REDACTED] to meet GSA's task order requirements. In some cases, a standalone task order-based [REDACTED] will be created, as needed.

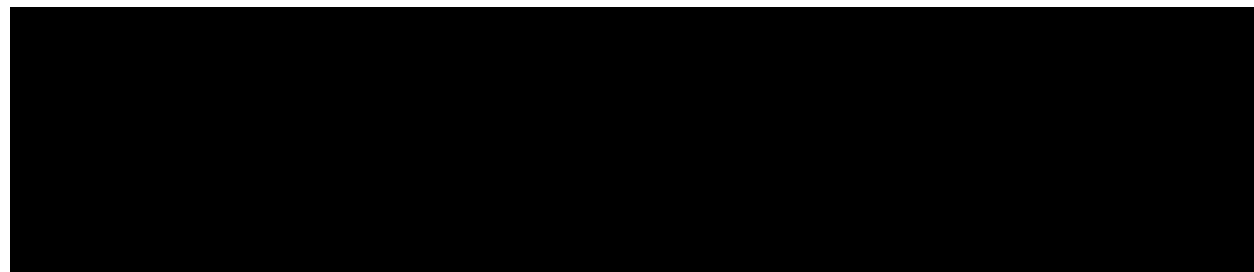


Figure 3.8.2.2.6-1. Task Order [REDACTED].

The Level 3 team will also identify any new training and awareness communications to ensure Level 3 personnel supporting the task order are aware of the new requirements and will be compliant with updated methods and procedures. This agile approach to task order-based [REDACTED] and dedicated oversight by the various functional teams will aid in minimalizing risks and adhering to the applicable guidelines.

3.8.3 Supplier Management and Quality Control

Level 3's EIS-MTIPS SCRM Plan contains stringent procedures for the selection of suppliers as shown in **Figure 3.8.3-1**, Level 3 has a defined process for selecting software, hardware or services in which multiple Level 3 organizational groups may be engaged in researching, vetting and approving new technology and/or suppliers. Level

3's [REDACTED] will invoke quality control measures and flows these down to OEMs, systems integrators and resellers to ensure [REDACTED] [REDACTED] Level 3 believes that this ensures we are well-positioned across the supply chain to execute supply chain integrity and oversight. As shown in **Figure 3.8.3-1**, various internal organizations may help to support the [REDACTED]



and return are included in all plans.

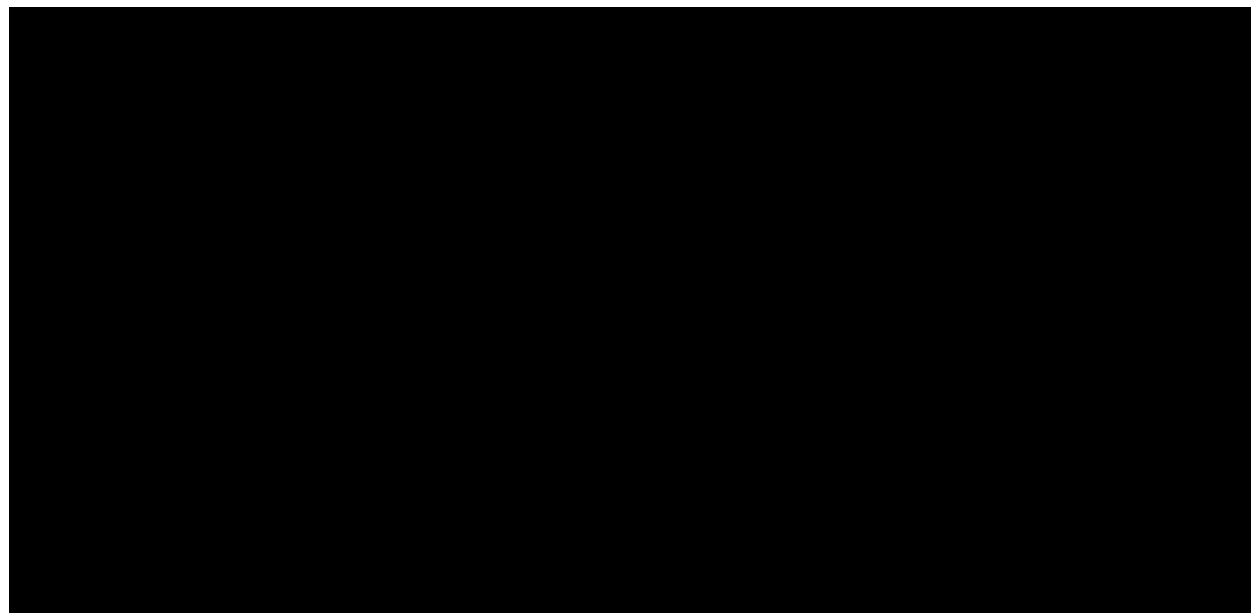


Figure 3.8.3-1. Supplier Selection and Approval Process.

Level 3 understands the challenges involved with acquiring new or replacement parts, components and software. It is of utmost importance to Level 3 that the [REDACTED]



process. Level 3 requires that resellers, OEMs or systems integrators have furnished Level 3 with their own [REDACTED]

[REDACTED] have been furnished to Level 3 and/ or our customers.

ensure risk is managed, controlled and mitigated prior to deeming system readiness. Level 3 will ensure key functional support areas work in tandem to manage risks by documenting potential threats, implementing risk mitigation steps, and holding suppliers accountable to their [REDACTED]

3.8.3.3 Security Control Implementation [L.30.2.2 (3), G.6.3 (3)]

The [REDACTED] plan will address the security controls for SA-12 (at least) as described in the NIST Special Publication 800-53 Revision 4 (**Figure 3.8.3.3-1**). The manner in which these controls are administered will be tailored in scope to the effort and specific information available at the time. Level 3 understands that individual task orders may vary from contract level requirements and may present unique circumstances and provisions that may require Level 3 to modify the implementation of such controls for GSA.

Figure 3.8.3.3-1. [REDACTED] Plan SA-12 Supply Chain Protection

[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]	[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]

3.8.3.4 Criticality Analysis (CA) [L.30.2.2 (4), G.6.3 (4)]

Level 3's key functional organizations and [REDACTED] will lead a Criticality Analysis (CA) effort, per NIST Special Publication 800-53 Revision 4 (or the latest published revision), that will develop processes and procedures to identify Mission Critical Functions supporting the contract level and individual task orders as part of the [REDACTED]. Mission Critical Functions will include, at a minimum, elements and components that comprise key infrastructure and systems that support the Level 3 EIS services requiring initial control baselines per NIST Special Publication 800-53, Revision 4 or the latest publication. Protection measures will be set in place to ensure system protection and mission effectiveness in supporting GSA's objectives. Several of the key functional teams involved in the CA effort may include SMEs from Corporate Security, Security Architecture Engineering, IT Development, Corporate Security, Vendor Management, Procurement, Network Operations and Business Development, along with other departments.

The CA team provides oversight for Level 3's key suppliers for hardware and software components supporting the [REDACTED]. The team's analysis will include proof of company ownership for key suppliers; to include their component manufacturers, precise locations of corporate offices involved in the supply chain and assurances from suppliers that system protection techniques (to include countermeasures and sub-countermeasures) are utilized on material and components supplied to Level 3. A close examination of each supplier's procedures will be conducted to determine quality control and safety of such material.

Level 3's CA efforts will be in place to minimize risk and to ensure GSA that the objectives outlined by GSA will not be impaired due to vulnerabilities in system design. The risk of sabotage or subversion of a system's mission critical functions or critical components will be rigorously protected and attacks will be thwarted.

3.8.3.5 Criticality Analysis (CA) Product and Component Quality Control [L.30.2.2 (5), G.6.3 (5)]

Level 3 will ensure that all suppliers will be contractually obligated to furnish Level 3 with documentation that ensures the authenticity and traceability of products which define the origination of such products and proof that they have not been subject to malicious intent during maintenance or repair. Level 3 will limit product acquisition activities to those OEMs and resellers that can ensure compliance with stated guidelines and agree to audits and assessments made by Level 3, the Government, or designated third parties, if deemed appropriate.

3.8.3.6 Criticality Analysis (CA) Supply Channel Monitoring [L.30.2.2 (6), G.6.3 (6)]

Quality control measures must be adhered to by suppliers of Level 3 and suppliers will be contractually obligated to agree to audits and assessments made by Level 3, the Government or a designated third party at any time, if deemed appropriate. Level 3 will validate components and products that [REDACTED]

[REDACTED]. Accurate packing slips, complete bill of materials, shipments being clearly marked and identified, packaging that follows the appropriate guidelines, examination of elemental damage to cartons, etc., will be reviewed and subject to inspection by Level 3 to ensure the flow of genuine products.

3.8.3.7 Logical and Physical Delivery [L.30.2.2 (7), G.6.3 (7)]

Documented methods, procedures and guidelines for purchase orders and for the receiving department are critical to ensure the smooth flow of goods from suppliers to Level 3. Processes will be set in place to assist in the successful and safe receipt of vendor equipment to the Level 3 stocking warehouses. [REDACTED]

[REDACTED]

Physical access to warehouses and staging areas will be closely guarded and monitored. Electronic delivery of software will also be protected and will fall under the access control list methods and procedures for adequate supply chain protection.

Level 3 will also evaluate the applicable suppliers' logistical methods and procedures to ensure that supply chain risk is avoided and well managed. For example, Level 3 will evaluate all suppliers' ability to oversee material goods and services during the timeframe between the purchase order issuance and the actual delivery timeframe in order to limit opportunities for adversaries to corrupt information system components or products.

Guidelines prescribed by Level 3 to the supply chain for [REDACTED] will include, but will not be limited to, the following:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Specific processes will be put in place that include step-by-step instructions to ensure strict quality control and access on a per purchase order basis. Protection mechanisms will look for evidence of:

- [REDACTED]

- [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

Processes will be set in place to ensure protection against the exposure of system components, information misuse, and unauthorized modification or redirection. Restricted access to warehouses and staging areas will ensure protection of system products and components. The reporting and documentation of supply chain issues that arise follow the following guidelines:

1. [REDACTED]
[REDACTED]
[REDACTED]

2. [REDACTED]
[REDACTED]

3. [REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.8.3.8 Operational Process [L.30.2.2 (8), G.6.3 (8)]

Level 3 recognizes that it is of critical importance to ensure processes are in place to protect products and components during maintenance, patching, element replacement and other sustainment activities. Only authorized and documented personnel will have the ability to access elements of the [REDACTED]

[REDACTED] Configuration management tools and patch guidelines will be followed in strict accordance with processes set forth by Level 3. All steps performed with patching and maintenance will be entered in a maintenance log, to be audited by Level 3 internal operations organizations as deemed appropriate. Disposal activities will follow a strict guideline to minimize unauthorized access to hardware, software and components. Careful labeling, tagging, tracking of goods that arrive and are disposed of by Level 3 will be documented closely to ensure the protection of the supply chain for all items that arrive and leave Level 3. Disposal procedures must be followed carefully to maintain the integrity of the network. Personnel will be trained on proper disposal methods and procedures, the consideration of permanent disposal of elements will be reviewed and authorized disposers as needed will be properly vetted to ensure the safeguarding of elements and data during the disposal effort.

3.8.3.9 Supplier Relationship [L.30.2.2 (9), G.6.3 (9)]

A Level 3 EIS Supplier Security Standard will be developed to ensure the selection of 1).OEMs, 2). Authorized resellers, or 3). Authorized partners/distributors. [REDACTED]

[REDACTED] All suppliers will be required to comply with the security standard set forth by Level 3 and will be required to agree to be subject to audits and assessments by Level 3 personnel. Clearly defined roles of each supplier will be identified. [REDACTED]

practices. Methods and procedures will be expected to be clearly identified by each supplier, as to limit counterfeit and illegally modified products from entering a suppliers' supply chain. Internal and external audits are expected to be conducted on a regular basis. Supplier reviews will be conducted to ensure:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3.8.3.10 Software Warranty [L.30.2.2 (10), G.6.3 (10)]

Level 3 will represent and warrant that (i) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.8.3.11 Verification and Validation [L.30.2.2 (11), G.6.3 (11)]

Level 3 will reserve the right to perform security compliance assessments and audits of supplier facilities, networks, environments or systems. In the event of a security incident, Level 3 may perform immediate audits of the affected facilities,

networks and/or environments, as deemed appropriate for all suppliers. [REDACTED]

[REDACTED]. In addition to assessments and verification activities, validation of such security requirements will be well documented.

3.8.3.12 Sub-Contractor Clause [L.30.2.2]

Level 3 will incorporate the substance of EIS RFP Section G.6.3 in subcontracts at all tiers where an EIS subcontractor provides personnel, components, or processes identified as [REDACTED]

3.8.3.13 Training and Awareness

Level 3's Training Organization will support the development and delivery of [REDACTED], and advise associated suppliers of the associated risks that could be involved in the supply chain lifecycle. Employees and associated suppliers will be required on an as-needed basis to participate in supply chain training programs and assessments run by their own organizations; respectively.

3.8.4 Plan Submittal and Review [G.6.3.1]

Level 3 understands that the [REDACTED], and when significant changes occur. All information as it is understood, will be treated as Controlled Unclassified Information pursuant to Executive Order 13556, shared only with Government agencies, and used

solely for the purposes of mission essential risk management. [REDACTED]

3.8.5 Definitions and Acknowledgements

3.8.5.1 Definitions

a) Level 3 understands that “Information Technology” (see 40 U.S.C. 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

1. For the purpose of this definition, Level 3 understands that equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires:
 - a. Its use or;
 - b. To a significant extent, its use in the performance of a service or furnishing of a product.
2. Level 3 understands that the term “information technology” includes computers, ancillary equipment (including imaging, peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.
3. Level 3 understands the term “information technology” does not include any equipment acquired by a contractor incidental to a contract.

Level 3 understands that “Supply Chain Risk,” means that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

- a. Level 3 will maintain controls in the provision of applicable supplies and services to the Government to minimize supply chain risk.

- b. Level 3 recognizes that in order to manage supply chain risk, the Government may use the authorities provided in section 806 of Pub L. 111-383. Level 3 understands that the Government may consider information, public and non-public, including all –source intelligence, relating to a contractor’s supply chain.
- c. Level 3 acknowledges that if the Government exercises the authority provided in section 806 Pub. L. 111.383 to limit disclosure of information, that no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.
- d. Level 3 includes the substance of this clause, including this paragraph (e) in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.