

## NNI Plan

Level 3 will build into both the Network and Security Operations Center (NSOC) and the Sam Houston Building (SHB) DIR facilities and provision electronics that will initially provide FE, GE, Wavelength, DS1, and DS3 interfaces. The initial requirement for colocation equipment will be two racks which will be provided and installed by Level 3 Communications and two 30amp/208v power, power will be provided by DIR. The initial capacity will be 1 GB and will be able to expand to 40GB. Additional fiber will be available so that if additional capacity is required all that will be needed is the addition of electronics. Level 3 will work with DIR to define agreeable thresholds on NNI utilization (as well as any additional critical links). The thresholds will be based on trending information (historical data) or additional DIR initiatives that project a significant increase. Level 3 will work to ensure that available NNI bandwidth will not become a bottleneck which would adversely impact DIR service performance.

In addition to the NNI infrastructure links, Level 3 will work to identify and monitor trends on the top utilized customer access circuits. During scheduled intervals for service reviews (monthly or quarterly), Level3 will provide a list of customer access circuits that are above a defined average utilization threshold (e.g. 75%). This will help in forecasting overall future network requirements and communication to our joint customers when they may be approaching utilization levels that could adversely affect their performance.

Level 3 strictly controls access to Level 3-owned equipment residing in DIR facilities. The statement of work defined for the construction at 1001 W. North Loop (NSOC) provides for the installation of a new wall mounted junction box (48"x48") to transition the 4" conduits coming in through the outside wall of the building. Level 3 technicians will extend a vertical EMT riser up to the existing ladder rack level, and 90 over onto ladder rack. The path will be extended with corrugated 1" duct from the new EMT path along the existing ladder rack over to the new transport rack location.

The statement of work defined for the construction at 201 E. 14<sup>th</sup> (SHB) provides for extending the Level 3 path with 1" corrugate duct, from the MPOE junction box over to the new rack location. This extended path is elevated at about 20' and will require special lifts to complete. Some ladder rack will need to be installed between the existing main path (laterally) to the new lineup location for the Level3 rack.

Assignment information for our gear in DIR facilities

Site	Floor	Room	Bay/Aisle	Cabinet Rack
E 14 <sup>th</sup> St., Austin, TX	1 <sup>st</sup>	Switch	Bay 1	First Available Cabinet
1001 N.W Loop, Austin	1 <sup>st</sup>	Equipment	Aisle/Row 2	Rack #5

## EXTERNAL NOTIFICATIONS - DIR

Level 3 maintains a 24 x 7 Security Incident Response Team that monitors and responds to unauthorized and suspicious activities within the Level 3 network and systems.

Should Level 3 Security Operations team identify an incident that is determined to have a security or integrity impact on a particular customer, Level 3 Security Operations will identify the customer security contact and attempt to notify that contact first via telephone, then via email. Level 3 Security Operations will then contact the Level 3 account representative to identify the appropriate notification contact if no security contact is listed or contact is not reached within a reasonable time.

## Level 3 Global Security Architecture

Level 3 is providing its Global Security Architecture Document in the following pages.

### GLOBAL SECURITY ARCHITECTURE



Level 3 Communications Global Security Architecture High Level Design Overview
--

<b>DOCUMENT NUMBER:</b>	L3GSA:IDSArch:01282001:01
<b>ISSUE:</b>	5.0
<b>FIRST RELEASE DATE:</b>	1/28/2001
<b>CURRENT RELEASE DATE:</b>	7/15/2009
<b>AUTHOR :</b>	Level 3 Security Architecture
<b>OWNER:</b>	Level 3 Communications
<b>AUTHORIZER :</b>	Dale Drew, Vice President

---

## Introduction

### Purpose

The purpose of this document is to provide a high-level overview of the security architecture considerations Level 3 has put into place for the protection of its production networks, systems and applications.

### Revision History

The table below chronicles the revision history of this document.

Revision	Date	Author(s)	Reason for Change
1.0	01/28/01	D. Drew	First Draft Release
2.0	3/20/04	D. Drew	Final
3.0	6/19/2007	D. Drew	Update
4.0	5/1/2008	D. Drew	Update
5.0	7/15/2009	D. Drew	Update

### Document Security

This document contains information classified **Level 3 Confidential**.

### Questions or Recommendations

If you have questions regarding this document or wish to recommend additions, deletions, revisions, or corrections to any security standards, processes, or practices in this document, contact:

Level 3 Global Security Architecture ([globalsecurity@level3.com](mailto:globalsecurity@level3.com)) c/o Dale Drew ([dale.drew@level3.com](mailto:dale.drew@level3.com))  
/ 720-888-2963

## Scope

This document contains the Security Concept of Operations (CONOPS) for the Level 3 IPVPN Wide Area Network (WAN). It provides a high-level overview of the WAN network infrastructure that is designed to securely support the service. This CONOPS shall define the architecture, capabilities, security posture, organization and responsibilities of the WAN and the interaction of the WAN with other networks within the Level 3 network.

The WAN system security includes the monitoring of all information about threats to international telecommunications networks, including the Internet. Countermeasures to threats are continuously updated as they are identified.

Figure 2-1 includes a high-level summary of the Level 3 WAN security threat concept.

Asset Protected	Threats	Countermeasures	Effectiveness
Gateway Facilities	<ul style="list-style-type: none"> <li>Unauthorized access</li> <li>Natural disasters</li> <li>Fire and accidents</li> <li>Malicious attacks</li> <li>Natural and other</li> </ul>	<ul style="list-style-type: none"> <li>Access controls, locks, and alarms</li> <li>Industrial-strength power and HVAC self-contained</li> <li>Extinguishing system, alarms, continuous monitoring</li> </ul>	Level 3 meets or exceeds industry standards* for physical security of facilities (e.g., limited access, biometrics, alarms, CCTV, back-up power, fire suppression, HVAC)
Network Systems	<ul style="list-style-type: none"> <li>Technical failure</li> <li>Unauthorized access</li> <li>Malicious attacks</li> <li>Natural and other disasters</li> </ul>	<ul style="list-style-type: none"> <li>Fail-over systems, continuous monitoring</li> <li>Access controls, firewalls, intrusion detection, and scans</li> <li>Systems security, continuous monitoring, recovery</li> </ul>	Level 3 has developed procedures that work toward achieving maximum availability and prevention of network attacks, and Level 3 meets industry standards* with physical and cyber protection. Not designed to resist attack of a determined adversary (e.g., military, terrorist).
Fiber-Optic Cables	<ul style="list-style-type: none"> <li>Accidental breakage</li> <li>Unauthorized access to signals</li> <li>Malicious attacks</li> </ul>	<ul style="list-style-type: none"> <li>Shielding and burial</li> <li>Technical difficulty and rapid detection of taps</li> <li>SONET rings and nets</li> </ul>	Built for resiliency and availability, the Level 3 system exceeds industry standards*.

Level 3 switching equipment Telecom carriers' equipment Collocation customers' equipment	<ul style="list-style-type: none"> <li>• Technical failure</li> <li>• Unauthorized access</li> <li>• Malicious attacks</li> <li>• Natural and other disasters</li> </ul>	<ul style="list-style-type: none"> <li>• Continuous monitoring, rerouting, and back-up systems</li> <li>• Physical security and network monitoring</li> <li>• Access control and response to alarms</li> </ul> <p>Note: Telecom carriers' equipment is stored in separate, secured spaces.</p>	Level 3 protections for the switching systems meet or exceed industry standards.* Resisting a determined adversary (e.g., a terrorist) would depend heavily on police response.
Authorized Personnel	<ul style="list-style-type: none"> <li>• Accidents</li> <li>• Fire, explosion</li> <li>• Malicious attacks</li> </ul>	<ul style="list-style-type: none"> <li>• Safety requirements and procedures</li> <li>• Fire suppression and detection</li> <li>• Physical security, monitoring, and response</li> </ul>	Level 3 protects customers and personnel as a primary goal, meeting or exceeding industry standards.*

**Figure 2-1. Summary of Security Threats and Countermeasures**

Updates are continuously made to the threat environment based on an assessment of the system-operating environment in terms of the five primary threat elements listed below.

- Natural Disasters, environmental and physical conditions that are not related to human actions (floods, volcano, earthquakes, etc.).
- System Failures, the result of malfunctions in any of the system components and are grouped into hardware, software, and communications link failures.
- Environmental Failures, the result of failures in the man-made environment of environmental control equipment (temperature, humidity, dust, etc.).
- Human Acts - Unintentional failures due to system and software design activities and failures resulting from system user action at all levels (Administrative, Maintenance Personnel, and Users).
- Human Acts - Intentional human acts against the system by authorized users and unauthorized personnel (hackers, vandals, thieves, etc.).

Threats are reviewed for all potential situations that could jeopardize the operation of services. The following contains information about the physical, personnel, and connectivity aspects of the environment.

---

## WAN Security Architecture Overview

Level 3 is committed to maintaining the security, integrity and availability of its networks. Level 3 operates an integrated security architecture managed by several dedicated security groups. These groups are responsible for providing protective measures for Level 3 commercial and internal networks, and provide a focus point for Level 3 customers to receive assistance on security related issues. These departments are:

**Security Architecture** – provides a focus for research and development in identifying, investigating, and testing newly discovered security threats, new security trends and security capabilities. This group is also responsible for the overall security architecture used to protect the Level 3 systems and infrastructure

**Security Engineering** – provides a focus for the development and/or purchase of security technology as well as the testing and integration of that technology into the WAN.

**Security Operations** – provides 24 x 7 monitoring and incident management response to all security threats

**Business Continuity** – ensures Level 3 has appropriate mitigation and disaster recovery plans in place. The responsibilities of these Security Departments are to identify and correct vulnerabilities that affect the commercial and internal networks, associated products and services and related support systems. Level 3 believes that early detection and analysis of security threats and exposures that impact the network is critical to providing a consistent assessment of the security level being provided. Level 3 Security Engineering and Operations focus to collect, identify, test, and correct security related events within the WAN network infrastructure. This process is designed, monitored and constantly upgraded to provide the best overall approach and to add technological innovations and accommodate industry trends and standards.

Level 3 protects over 46,000 systems across six physically distinct networks. They monitor and mitigate approximately 900,000 intrusion attempts every day against the network. Every element in the network, from production systems to desktops, are audited every 24 hours to verify compliance with policies and threats to integrity.

Level 3 employs an “Envision, Engineer, Operate and Respond” lifecycle that provides a continuous capability to ensure processes and systems are optimized to their fullest extent. An engineering and architecture group is maintained that is responsible for the research, development and integration of security mitigations solutions within the network architecture. In many cases, this involves an analysis of off-the-shelf security products, to identify “best-of-breed” solutions. The group focuses much of its effort on analyzing best practice models to identify enhancements or new capabilities to the security architecture.

Level 3 regularly conducts security review meetings with industry peers and law enforcement agencies to identify the latest trends and movements within the security arena. This ensures current, proper practices are in place within the network.

Level 3 maintains a Security Engineering lab used to provide an evaluation and assessment function to the Security Engineering Department. The Security Lab is used to regularly review commercial security products and performs assessments on the network, systems, and applications, as well as functions to test and verify application code used within the infrastructure.

The Security Lab plays a critical function in keeping the Security Engineering Department up-to-date on security issues that may have an operational impact on the network.

Level 3 has a comprehensive security infrastructure in place to provide a cost effective and flexible security infrastructure that can quickly adapt to current and evolving threats.

### **Security Policy Architecture**

Level 3 has an extensive security architecture framework, used to ensure success in the deployment of its security policy. The Security Architecture vision statement is:

Level 3 uses the International Organization of Standardization ISO 17799 standard as its security policy framework, with specific guidelines and practices mapped into that standard that assist in setting the

direction and expectations for compliance. These guidelines are based on industry best practice models, including sources from:

- Federal Communications Commission Network Reliability and Interoperability Council (NRIC FG1B).
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG).
- Internet Engineering Task Force (IETF) site security RFCs.
- Third party audits.
- National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems.

Level 3 uses these policies and regulations as the basis for its security policy and the security standards derived from that policy provides specific configuration guidelines that are designed to ensure the network is operated in a secure manner. These standards are used to ensure the network is in compliance with federal guidelines and that it is monitored in relation to these security standards. The security policy sets the foundation for protecting the network by outlining procedures for providing a cost effective and flexible security infrastructure that can quickly adapt to current and evolving threats:

Identify risks and evaluate their potential impact:

- Collect intelligence for lab analysis.
- Review security products regularly.
- Conduct inventories of network, system, connection, and data assets.
- Conduct audits on the network, configuration, applications, and host.
- Monitor for exposures and suspicious activity.
- Ensure accountability and rights management of all activities on the network.

Enable users through technical and policy controls:

- Maintain policies and standards to set expectations.
- Promptly and openly address specific issues and concerns.
- Directly provide security capabilities to the end user to optimize security functions.
- Minimize the perceived "barrier" to security thus making it seamless and understandable as possible.
- Pursue areas of constant improvement and optimization.
- Support two factor authentications where ever possible.
- Ensure the principal of least privilege when accessing information resources.
- Ensure the proper level of logging for system activities.
- Protect data and information resources from unauthorized disclosure.
- Support appropriate levels of redundancy and integrity of business continuity.
- Enable designs to support non-repudiation principles.
- Ensure the proper levels of protection are in place between information resources.

Level 3 then implements security technology and process controls to measure compliance to these practices.

The model foundation is based on ensuring security is covered at the following layers illustrated in Figure 3.1-1:

- Transport
- Network
- System
- Applications
- Data
- Users

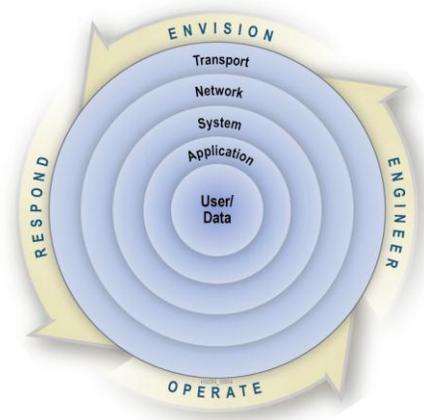


Figure 3.1-1. Security Policy Model Foundation

In addition, the model provides for compliance coverage in the following areas:

- Authentication
- Authorization
- Accounting
- Confidentiality
- Availability
- Integrity
- Trust Domains

### Security Infrastructure

All security systems identify compliance with applicable Level 3 security standards, and assign identified vulnerabilities with one of five security severity ratings; each with a specific remediation SLA:

Type	Description	SLA
Severity 5	Improperly installed or non functioning security tool	24 hours
Severity 4	Severe security exposure within perimeter or internal network that could lead to admin/root/domain level access to a resource.	Immediate. Blocking/filtering/protection efforts to protect while mitigation in progress.
Severity 3	Critical security exposure within perimeter or internal network that could lead to user/application level access to a resource.	One week
Severity 2	Compliance violation of security guidelines	One quarter
Severity 1	System configuration not in compliance with best practices	As time permits

The Level 3 security infrastructure is designed to provide the highest level of security to the network by providing a comprehensive risk management security architecture that ensures countermeasures are

continuously monitored and upgraded. The security infrastructure consists of the following functional components:

### **Audit/Detect Infrastructure**

- Daily host and application audits via security agents are installed on all employee and production systems within the network.
- Daily configuration audits from a central network element data store.
- Daily network vulnerability scans against all elements.
- Real time monitoring of unusual, suspicious or unauthorized events on the service in near real time.
- Fraud monitoring systems that identify and perform an analysis of Session Initiation Protocol (SIP) signaling and Call Data Records (CDR) data to detect potential fraudulent voice calling patterns

### **Inventory Infrastructure**

Daily inventories of all active MAC addresses, IP addresses, interfaces, systems, applications and network connections identify the deployment of new systems and changes to existing systems. A daily inventory of all production and employee elements is performed.

The inventory includes:

- Validation that security tools are properly loaded and configured.
- Collection of system architecture information.
- Collection of network interface information.
- Collection of what processes are running and what resources they are utilizing.
- Collection of what network connections the applications are utilizing (for risk relationship analysis).
- Monitoring all commands executed on production systems.

### **Security Identify/Evaluate Infrastructure**

Level 3 collects industry vulnerability threat information from over 2,000 public and private sources used to identify new exploit releases, patch availability and security threat trend information. This data is then correlated and given a severity ranking for analysis within the security lab to identify the scope of impact.

Level 3 also maintains an extensive network of passive probes and collectors used to forensically analyze network attacks for trends or new exploit releases that may impact the network.

### **Protection Infrastructure**

All production elements are protected via two-factor authentication or are deployed behind bastion hosts that require two-factor authentication.

### **Firewall Infrastructure**

All perimeter and high value networks are designed with a firewall layer.

### **Denial of Service detection and mitigation infrastructure**

The Level 3 network is monitored by an automated system to trace Denial of Service attacks in progress.

### **Rogue detection and quarantine infrastructure**

Systems that have access to the corporate OSS network that do not comply with security tools policy are automatically moved to a quarantine network where the system is isolated from the production environment.

### **Security Enablement Infrastructure**

A lab exposure scanning system enables system owners to scan their systems prior to deployment in the production network. All systems are required to be scanned and all critical exposures to be repaired prior to deployment.

### **Security Assess/Reporting Infrastructure**

All identified security exposures are dispatched to the alarm display system within Security Operations and also sent to a web based vulnerability-reporting server that allows Element Owners to access and identify information about the security of their systems.

### **Security metric reporting system**

Security Metrics are calculated automatically and represent the security health of the network. Metrics include:

- Tool deployment ratio – ensuring security tools are properly deployed and working.
- Severity ratios – identifying security exposures that exist on systems in each SLA category.
- Top areas of improvement – classes of system or element owners who “own” the highest level of exposures.

### **Exposure Analysis**

Level 3 has developed a customized Exposure Analysis (EA) infrastructure designed to provide for the utmost in stability relating to its impact on the network. This infrastructure has a number of safeguards to ensure minimal impacts to the production network will be realized, even under the most severe cases.

A more aggressive exposure analysis scanner exists in the Network Engineering lab. The objective is to ensure boxes are thoroughly tested before a new piece of equipment or software is deployed in the production network. Performing a proper security risk assessment on elements before they are deployed into production is critical to ensuring the integrity of the WAN.

The testing process attempts to utilize as much automation as possible, to minimize the total impact to the tester; while at the same time ensuring enough information is collected on the capabilities of the element being tested for a proper risk assessment.

### **Risk Assessment**

The risk assessment process will cover the following areas:

- Registration. Security Architecture maintains a risk assessment registration system that is the primary vehicle for gathering information on the security capabilities of the element in relation to required security policy.
- Assessment. The element can then go through a network based risk assessment system to identify critical security exposures.
- Specific Assessment. The Level 3 Security Standards document describes specific security requirements for some elements that need to be validated prior to rollout.

### **Element Registration**

The process applies to anything that is getting deployed into the production network: applications, systems, network elements, vendor product, and internally developed systems and applications. The goal is to have all such elements registered with the Security Risk Assessment system. Upgrades to already registered elements do not need to be re-security tested, unless there are significant upgrades in functionality and/or behavior to the element.

All testers are required to register their testing activity with the 3Guardian Information Assurance Security Registration System.

One of the import aspects of a proper security risk review is to register the element that is being tested with the 3GuardianIA Security Registration System. This system walks the user through a security questionnaire to identify the level of security capability the element has. These questions represent the Security Standards requirements for all elements within the Level 3 network.

The registration system will then assign a "Risk Rating" and it will be sent to a Security Engineer, if necessary, to further examine those risks that are deemed significant and need to be repaired prior to deployment. The Security Engineer will work with the tester to identify mitigation strategies to repair any identified risks before the element is production deployed.

### **Automated Scanning (ScanMeNow)**

The ScanMeNow system utilizes a series of network based security scanning tools that will be run against the system automatically to identify possible areas of remotely exposed risks. The scanner will utilize buffer overflow checks, denial of service checks and other network based checks. The element should be monitored during these tests to identify possible impacts that are not immediately detected by the scanner.

All testers are required to utilize the "ScanMeNow" to test an element to identify remote network exposures.

The tester is emailed a web link to the test results when the scan has been completed. Test results are color coded by Red, Yellow and Green; red items must be repaired prior to production deployment.

### **Specialized Scanning/Testing**

The 3Guardian IA Security Standards Document lists specific security configuration and protection requirements for specific classes of elements in Appendix A of the 3Guardian Information Assurance Security Standards Document. All specific elements that are listed in this appendix need to be specifically tested for those listed requirements prior to deployment.

If specific testing tools or methodologies are needed to successfully complete the tests, the Security Architecture and Engineering group is contacted for assistance.

### **WAN Security environment**

Level 3 has developed several dedicated network security groups that specialize in corporate security and security policy. These security groups also are involved in the security architecture and engineering of the WAN by developing the security infrastructure, being involved in the overall design of the network, and by ensuring that the security standards set for the network are current and adequate. Members of these security groups are also responsible for manning the Security Operations Center (SOC) that monitors the network 24 x 7.

### **Network SOC**

The Level 3 SOC is staffed and operational 24 hours a day, seven days a week. The SOC is responsible for monitoring the network to ensure that it is operating properly and securely. The goal of the SOC is prevent, detect, and respond to any and all threats to the network. If a threat is identified then the SOC is trained to contain, monitor and mitigate the threat. Once the threat no longer requires mitigation, the SOC is responsible for the recovery of the network. The SOC performs and provides the following functions:

### **Security Assessment Tools**

Level 3 has developed and uses tools that protect and ensure that the network is secured and not exposed to threat agents that could jeopardize the confidentiality, integrity, and availability of the network. The security assessment tools include but are not limited to the following:

#### **Inventory Tool (IT)**

The inventory tool function is to generate a network inventory snapshot of the production network. It does this by ping scanning all network IP addresses and interrogating responsive elements to determine the

element vendor, model, version, and network configuration. The inventory also identifies security tool coverage, and identifies system interfaces to summarize servers connected to the network with multiple interfaces.

#### Process Inventory and Trending Tool (PITT)

The process inventory collects process and logging information for production applications and their network relationships. It is designed to inventory production applications and user utilities by:

- Collecting a list of all running processes on all production systems.
- Collecting a list of all application network associations and then fingerprinting those applications.
- Registering new applications by automatically contacting the application owner.

This data is collected in order to:

- Add application owners into the Security Vulnerability Reporting system.
- Identify when new, non-security approved applications enter the network.
- Review security capability of applications to build compliance tools.
- Feed vendor information into Intel collection systems to identify published security issues.
- Collect security related logging data.
- Identify when significant behavior changes with an application.

#### Host Assessment (HA)

Host Assessment is a collection of internally developed tools designed to work within either the Unix or Windows environment. A central server schedules assessments on clients based on a pre-determined schedule. This server performs integrity checks on the client to ensure that it has not been tampered with before the assessment is conducted. The client monitors the health of the system before and during the assessment and pauses or shuts down if the system is impacted.

All results are sent to the central server for analysis. The central server ensures data is being collected and the results are sent to the Collection, Alarm, and Reporting infrastructure. Figure 3.3-1 is a diagram of the HA process.

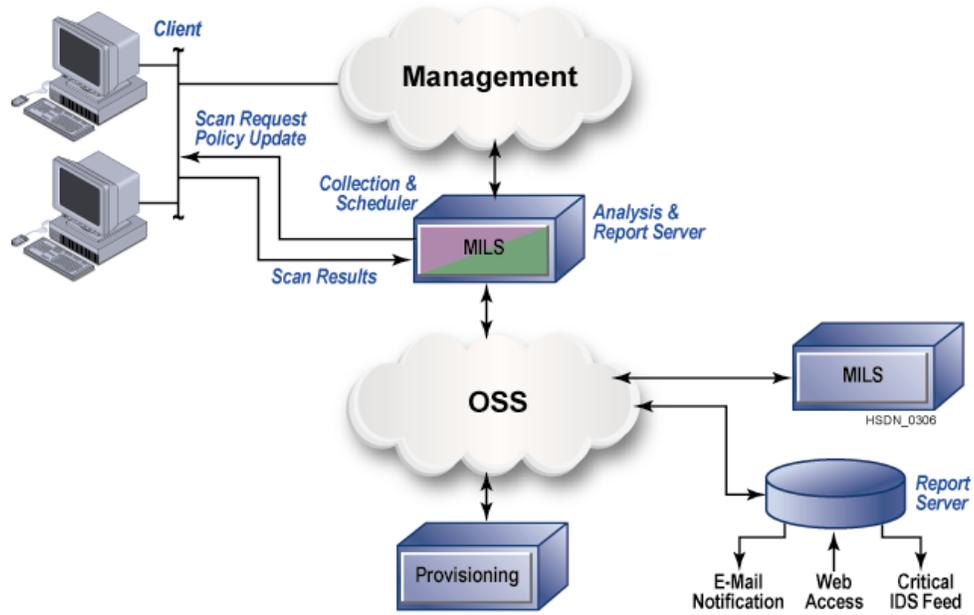


Figure 3.4-1. HA Process

Configuration Assessment (CA)

The primary function of the CA security tool is to validate policy compliance on network elements. The CA tool is an internally developed tool that use XML based templates to audit configurations and identify security non-compliance. Configurations from production and internal equipment are copied to the security configuration system and the results are analyzed and sent to the collection, alarm, and web reporting system. Figure 3.4-1 shows this process.

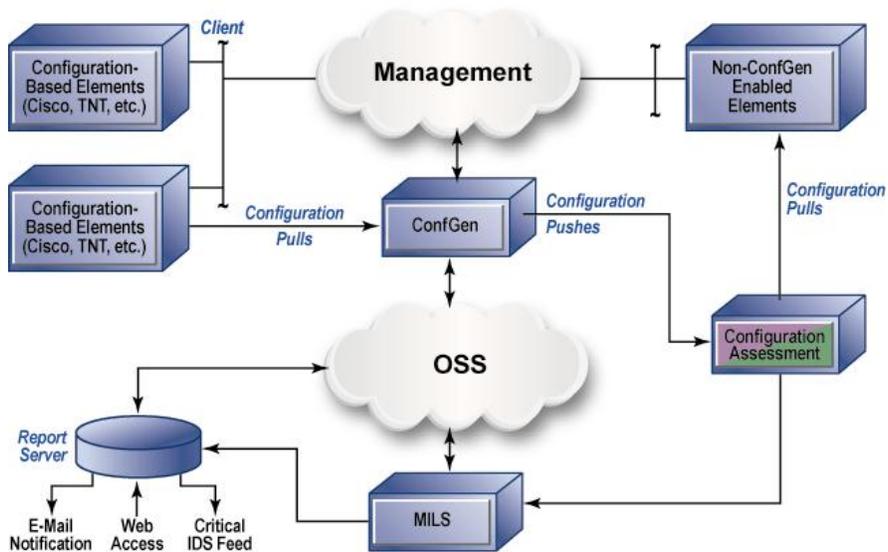
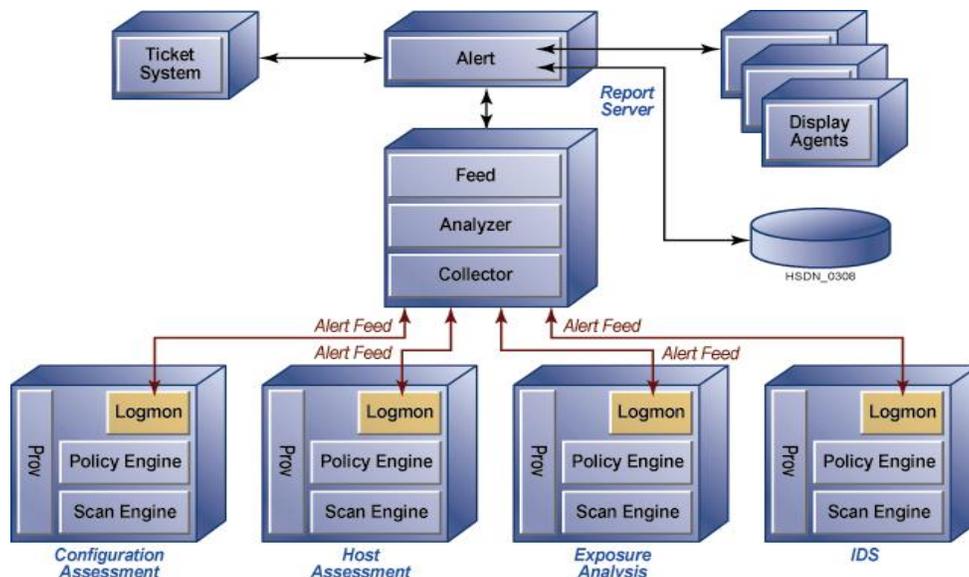


Figure 3.4-2. CA Process

**Intrusion Detection Client**

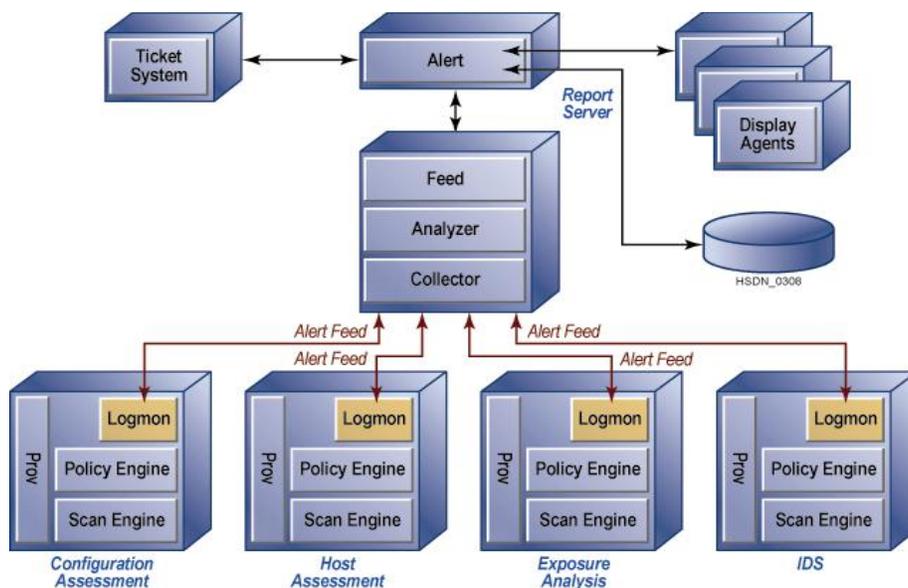
The intrusion detection client is an internally developed client-based agent that collects data from OS and application events. This security tool monitors for messages that match pre-defined patterns for specific files, events, and classes of systems. The intrusion detection client monitors CPU memory and will suspend operation until the system load is below defined watermarks. All data collected from the host intrusion detection system, firewalls, network intrusion detection system, and other security devices are forward to a central server for analysis. Figure 3.4-2 is a diagram of this process.



**Figure 3.4-3. Intrusion Detection Client**

**Intrusion Detection Server**

The intrusion detection server is a policy engine designed for near real-time event monitoring. It is a highly distributed client/server model designed to be modular. The intrusion detection server performs correlation and investigative or research analysis. All data collected is forwarded to the Security Operations Center. Figure 3.4-3 is a diagram of this process.



**Figure 3.4-4. Intrusion Detection Server**

### Network Exposure Analysis (EA)

The primary function of the network exposure analysis tool is to remotely scan IP systems to find security exposures. It is an internally developed solution based on open source tools such as Nessus. Its current deployment is a cluster-based architecture that schedules a network scan for a particular set of cluster clients. This infrastructure repeatedly and continuously scans the network and the results of those scans are sent to the collection, and alarm, and web reporting system. Figure 3.4-4 shows this process.

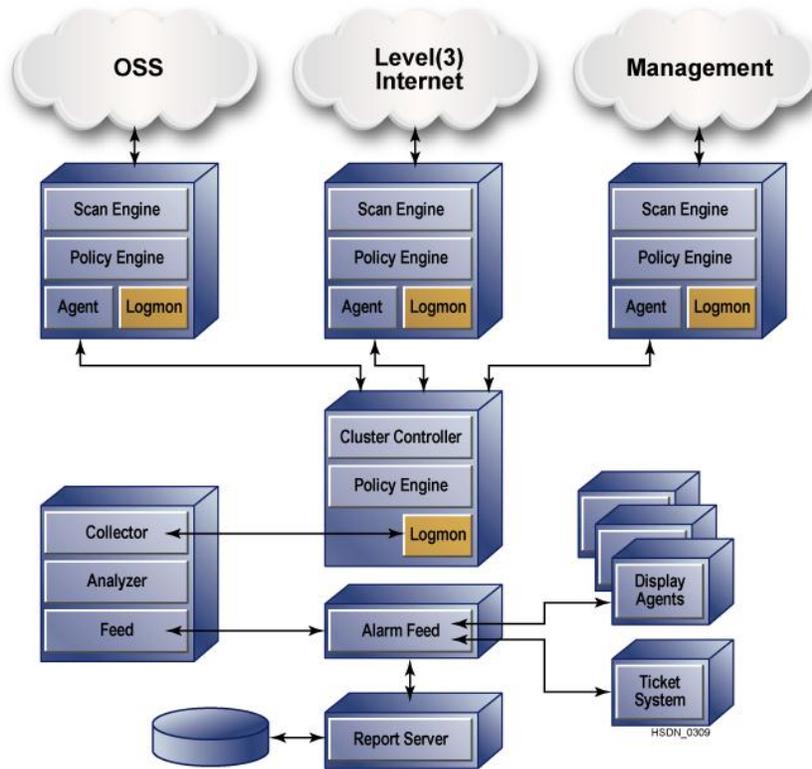


Figure 3.4-5. Network Exposure Analysis

### WAN Connectivity

The WAN connections to all domains are tightly regulated. All systems connecting to the WAN must be accredited and meet all the security requirements for accreditation before they will be allowed to connect.

### Connectivity

Hypothetical WAN connections are illustrated in Figure 3.5-1.

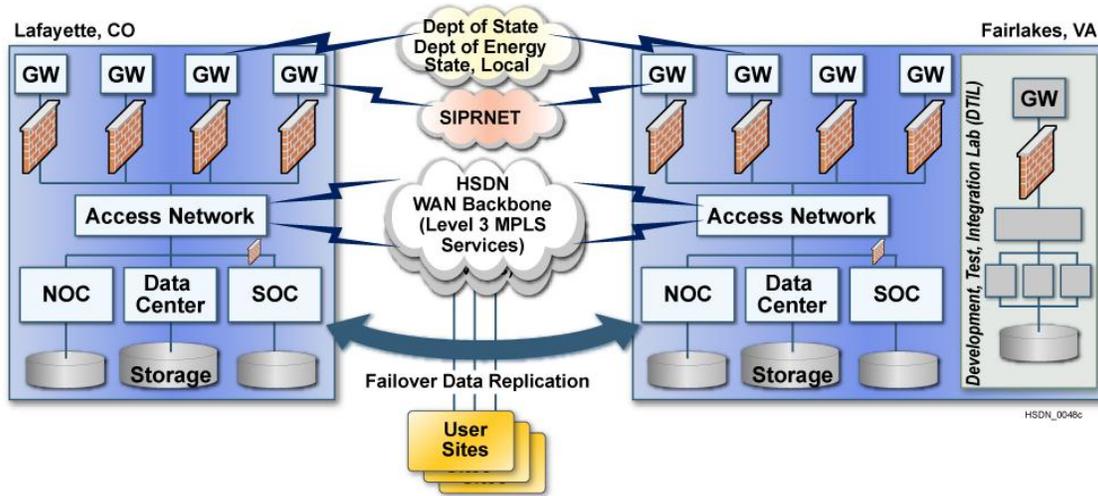


Figure 3.5-1. WAN Site Connectivity

## Logical Risk Management

### Protection against Denial of Service

Level 3 is particularly aware of the potential for denial of Internet service due to malicious attack. Through continuous network monitoring, Level 3 detects and responds to problems immediately, whatever their cause.

Level 3 is equipped to detect service-affecting intrusions. If, for example, a customer requires assistance, Level 3 can apply mitigating controls specifically to hostile traffic. With this capability, Level 3 can apply controls near the affected customer's interface with Level 3. These controls are applied for the time necessary to ensure normal service levels are restored and maintained. Their use is coordinated closely with the customer, and the result is often immediate mitigation of the attack.

Level 3 goes "above and beyond" industry standards by requiring all management of the network is done via an out-of-band management network. Network devices cannot be managed via the in-band signal. Access to the out-of-band management network is authenticated with a two-factor methodology: one-time user authentication codes in combination with personal identification numbers.

Through its host- and network-based intrusion detection systems, Level 3 has the ability to evaluate any intrusion or outage in near real-time using security experts in the SOC. If an intrusion were to affect service, an escalation procedure ensures the proper level of technical expertise for the event. Many events do not require escalation as the procedure defines immediate corrective action. The customer is kept informed by both their Technical Customer Account Manager (TCAM) and network security operations personnel as an event is detected, addressed, and resolved. These contacts occur immediately, by telephone and e-mail. Level 3 reviews logs and device performance on a continuous basis.

Security controls to protect against logical attacks and unauthorized access or usage include:

- Kernel and stack modifications to enhance network element resistance to denial of service attacks.
- Disabling of potential risk in transport, such as IP redirect, malformed packets, and packet relay services.
- Access control configurations that allow access only to authorized users of the element(s).

- Protection of all elements with strong authentication. Where strong authentication is not possible, elements are only accessible from elements that support strong authentication.
- Real-time monitoring of all elements for anomalies, attacks, and unauthorized behavior or usage.

### **Security Engineering Department**

Level 3 maintains a Security Engineering Department that is dedicated to researching new attacks, attack methodologies, vulnerabilities, and security compensators. The group also develops and maintains a security infrastructure for Level 3 production systems. The team proactively collects and analyzes new security threat information in a variety of ways, including the following:

- Security mailing lists (bugtraq, ISN, Firewalls, plus 54 others).
- Security advisory lists (CERT, CIAC, AUSCERT, plus 17 others).
- Industry Security Advisory Groups (ISPSEC, FINNA, CSI, plus five others).
- Federal Security Advisory Groups (NSTAC, NSIE, IRSCIS, plus three others).
- “Security Underground” sources.
- Manual research operations for “deep-dive” analysis of security exposures.
- Patch Management

Level 3 automatically collects and analyzes security-related data from multiple sources to identify new threats, security product news, and security patches. This data is collected from more than 2,200 sources on a daily basis, including mailing lists, news groups, Web sites, ftp sites, and chat rooms. All threat data is collected and analyzed for potential exposure in a network-engineering lab. Once compensators have been identified, they are deployed in the field.

---

## **Business Continuity Plan**

Level 3 Business Continuity Planning methods and procedures cover the most likely equipment failures and service disruptions. The Business Continuity Plan strengthens these procedures, and includes three major components:

- Risk Management Program
- Emergency Response
- Business Resumption

### **Risk Management Program**

The ongoing Risk Management Program calls for preventive measures that reduce the likelihood of disaster — and minimize the impact if one does occur. Under the Risk Management Program, there are four major areas:

- Potential threats - Natural, environmental, or incited, and threats that can affect the security and operation of a facility
- Key risk areas – Areas that have a significant impact on critical business functions and high exposure in the event of disaster. These key risk areas include utilities, communications, data processing equipment, and critical records
- Responsible parties for the management of preparedness and prevention activities
- Recommendations for preventive measures

### **Emergency Response**

The Emergency Response Plan includes guidelines for the initial response to crisis situations, primarily for management to use during damage control and disaster recovery. With team structures defined, the Emergency Response Plan addresses situation assessment, activation and notification procedures, operational and security response, and media communications. As with the Risk Management Program,

the Emergency Response personnel conduct routine exercises quarterly and update the Business Continuity Plan as accordingly. Examples of exercises conducted, but not limited to:

- Workplace Violence
- Network Outages
- Hurricane Management & Response
- Trans-Atlantic Cable Cuts
- Trusted Insider Cyber Exercises

### **Computer Emergency Response Team (CERT)**

The CERT is the single focal point for an incident. The team translates the technically oriented assessments of the trusted agents and on-site handling team into potential management directed responses. Based on management guidance, the team oversees response implementation and provides status updates. The team also interfaces with corporate marketing, legal, human resources and law enforcement as necessary. The team is composed of experts from GSO, Security Engineering, and Security Operations Management. The team lead is determined by the nature of the incident.

### **Incident Handling**

As security incidents occur, management will react to protect the information resources. How security incidents are handled can have a profound effect on their impact to the network. No plan can handle every contingency so to assist customers Security Engineering can assist system owners to provide a compiled security assessment for their specific environment.

### **Goals**

When a security incident occurs, a set of goals is determined for the handling of the incident. These will help to determine the Level 3 position for handling the incident (Proceed and Protect, or Pursue and Prosecute). Possible goals are:

- Assure the integrity of critical systems.
- Maintain and restore data.
- Maintain and restore service.
- Avoid escalation and further incidents.
- Avoid negative publicity.

These goals must be prioritized to form a response. Data is considered more important than hardware, application programs, or operating systems as these can all be recovered. Any steps taken in response to a security incident will be prioritized using the following guidelines:

- Protection of human life and the safety of people.
- Protection of sensitive or confidential data.
- Protection of other data.
- Prevent damage to systems.
- Minimize disruption to information resources.

### **Containment**

Containment of the problem should be the first step of a response to a security incident. The best approach to containment of the incident must be determined and acted on. This may include shutting down the information resource, removing it from the network or deploying protective measures around the effected resource (such as a firewall). Therefore, management fully supports all efforts to contain the incident and contingency planning includes security incidents.

### **Monitoring**

When the incident has been contained, the cause must be identified and stopped. All systems affected must be examined for evidence of the incident.

### **Eradication**

When the incident has been contained, the cause must be identified and stopped. All systems affected must be examined for evidence of the incident. Any changes must be corrected and the system returned to its normal configuration. Additionally, any backup media of the affected systems should be examined to determine their state. Eradication involves a complete review of the system and may be time consuming. Security tools may be used to speed the process. The Level 3 CERT will work with the system owner to review log data, perform a vulnerability assessment against the system and assist in protecting and patching the system.

### **Recovery**

The recovery process consists of returning the system to its normal state. Additional security patches or fixes for the vulnerability exploited may be employed. The system should undergo a complete backup and only then be placed back into production.

---

## **Maintenance Support and Operations**

### **Detailed Description of Function**

The Scheduled Maintenance process covers the notification and management of scheduled maintenance activities on the Level 3 network. Level 3 will pro-actively notify each other of service affecting and potentially service affecting maintenance. Each organization will track their non service affecting (NSA) maintenance internally so that it can quickly be referred to in the event that it unexpectedly begins impacting services.

### **Definitions**

**Scheduled Change or Maintenance:** A Scheduled Change is a change that is proactive and can be planned in advance and in adherence to the defined lead-time for types of changes. Most changes are Scheduled Changes and follow the conventional change process.

**Demand Maintenance or Change:** This type of change is defined as an immediate need to make changes to the current state of the environment. The environment is “demanding” prompt action to correct a high-risk condition. The immediate need should be directly related to an outage, potential outage or degradation and there should be an existing Problem/Incident case open to correlate the change request to. Such changes may require emergency approval outside of the GCR or may gain emergency approval through the Change Escalation process

**Escalated Change:** The Escalation process is initiated whenever defined standard intervals cannot be met. Such changes are planned with less than 21 full calendar days lead-time. Director approval is required on all expedited maintenance requests. Escalated requests will be assessed for customer and network impacts final approval being granted only after Operations Engineering, CMT, TCAM, NOC & GSM department heads have adequately reviewed the maintenance activity in question and considered the urgency for implementation.

**Emergency Change:** An Emergency Change request fixes a serious and impacting production broken situation, prevents an immediate problem that will stop production, or protects Level 3 from significant negative revenue impact. Such changes must be implemented outside of the normal approval process and require emergency approval from the members of the GCR.

## Scheduled Maintenance Classifications

**Service Affecting (SA):** Service Affecting changes directly impact the service of Level 3 internal or external customers.

**Potentially Service Affecting High-Risk (PSA-High):** PSA-H changes have a high potential of impacting the service of Level 3 internal or external customers, even if no impact is expected. These changes are often more complex in nature and thus incur more risk to the environment. (e.g. work on a different fiber in the same tray as the fiber carrying the backbone service for the IP network)

**Potentially Service Affecting Low-Risk (PSA-Low):** PSA-L changes have a low potential of impacting the service of Level 3 internal or external customers, even if no impact is expected. These changes are generally less complex in nature and incur less risk to the environment. (e.g. work in a different fiber tray as the fiber carrying the backbone service for the IP network)

**Non-Service Affecting (NSA):** Any change that has absolutely no possibility of impacting the service of Level 3 internal or external customers is considered NSA. This is a very limited scope of work and is often considered standard operating procedure.

## Network Maintenance Windows

Maintenance Windows are considered to be local time of area impacted. This is the only time in which that particular type of maintenance is allowed to occur. If multiple regions or time zones are impacted, the eastern-most regional time zone will determine the start of the maintenance window.

### Maintenance Windows – Most Network GCRs:

Classification	Days of the Week	Local Time
SA	Monday - Sunday	00:01 – 06:00
PSA-H	Monday - Sunday	00:01 – 06:00
PSA-L	Monday - Sunday	00:01 – 06:00
NSA	Monday - Sunday	Not Required

### Maintenance Windows – IP-Related GCRs:

Classification	Days of the Week	Local Time
SA	Monday - Sunday	03:01 – 06:00
PSA-H	Monday - Sunday	00:01 – 06:00
PSA-L	Monday - Sunday	00:01 – 06:00
NSA	Monday - Sunday	Not Required

---

## Technical Controls

### Router Administration

Network routers are administered in accordance the Level 3 Security Policies and Procedures and Change Management Procedures. Routers are configured to only support the services and protocols needed by the network to meet operation commitments (deny by default).

Access to WAN routers is only given to pre-authorized individuals. Authorization is based upon business function, meaning that access profiles are automatically assigned to a user based on the support function the user needs to perform. Access requests are authorized by the requestor’s manager and approved by

the owner of the network element. Oversight of this function and all exception approvals is provided by the Security Operations Office.

Access to routers is only allowed from pre-authorized locations and must a strong authentication mechanism.

Change control to routers is formalized via the WAN Change Control Request. All change control requests must include:

- Impact analysis & Customer notification period
- Dependency layer analysis
- Lab tested maintenance activities to be preformed
- Back out plan
- Stakeholder review and approval

All WAN router elements are backed up on a daily basis and audited to validate adherence to the change control process and to identify possible security exposures.

## Identification and Authentication

Level 3 enforces individual accountability by requiring the capability to uniquely identify each user to the system and then requiring users to identify themselves before beginning to perform any actions that the system is expected to mediate. The system elements will protect user authentication by limiting invalid login attempts and preventing unauthorized access to authentication data.

Network elements require trusted users to login prior to assuming a trusted profile (e.g., System Administrator, user) where each trusted user is uniquely identifiable (e.g., user name or other user id) within any administrative domain. All network elements utilize a two-factor one time password authentication mechanism for authentication access.

Network elements provide the capability of authenticating user identities and of associating a user's identity with all auditable actions taken by that individual. Users may be authenticated by password (trusted user) or token (general user) supported by the element. Group authentication will only used in conjunction with a unique individual authentication, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator. Any use of group authenticators must be explicitly approved by Level 3 Security Engineering.

## Availability

Network system elements are capable of detecting and logging the failure of system services or resources. Normally the WAN system elements will also provide the capability to generate a notification to a trusted user upon failure of a system service. The type of failure and the time of the failure will be logged to system audit files and normally sent as a message to the console of an administrative and logging system. Upon recovery of a failed system resource, the server will verify that it returns in a secure state; that file systems are intact; that access control permissions are unchanged from the state prior to the failure; and that privileges have not increased.

## Access Control

Network elements provide the capability to create, maintain, process, and protect an audit trail of access and significant security events from modification, unauthorized access, or destruction. The elements will provide the capability for a trusted System Administrator to define significant security events and to

enable or disable auditable events and provide enough information within audit records to allow an investigator to understand the auditable event.

Generally, the information includes the date and time of the event (e.g. common network time) the system component and process that initiated or completed the event, and the action involved.

Audit records are periodically backed up and archived onto different system or media than the system being audited. Archived records are reviewed and maintained in accordance with site-specific policies and procedures.

Level 3 has the capability to monitor audit trails, in real time in many cases, for occurrences or accumulation of auditable events that indicate security policy violations, and the capability to correlate system administrative and audit logs and to apply audit reduction and analysis tools to facilitate review and generate reports.

## **System Integrity**

Network elements employ procedures or technical configuration management controls to validate, periodically, the correct operation of the hardware, software, and firmware elements of mechanisms enforcing system security services. Additionally, the WAN system elements employ procedures and technical system features to assure that changes to component security services and supporting security data are executed only by authorized personnel or processes and are properly implemented (both during normal operation and during recovery from failure).

Security Engineering has employed software that detects the introduction of malicious code and will be managed to ensure the timely updating of protective software (e.g. updating anti-virus software). Administrators are required to follow these guidelines to protect the systems: all users use malicious code protection software to prevent, detect, and eradicate malicious code.

Files downloaded from another system are scanned immediately for malicious code. Diskettes received from other users or organizations as well as shrink-wrapped diskettes are scanned for malicious code prior to use.

Programs discovering malicious code on any media automatically report the discovery to the SOC. The support systems are maintained with up-to-date virus protection software. Signature files are updated on a periodic basis.

## **System Security Review and Oversight**

Level 3 utilizes ISO 17799 as its Information Assurance policy infrastructure. Security Standards are then mapped to each policy directive, with a policy owner identified for each directive.

Technical Control Security Standards are reviewed on a bi-annual basis to identify any possible changes that need to be added to the standards infrastructure. This analysis is based on:

- Lessons Learned analysis from CERT response activities
- Review of industry best practices
- (Network Reliability and Interoperability Council) NRIC FG1B
- DISA Security Technical Implementation Guides (STUG)
- Other best practices (IETF RFC, NSP-SEC, etc)
- Analysis of threat collection data.
- Output of third party audits.
- Feedback from strategic and tactical security meetings with business units within the company.

All network elements must go through formal security lab testing and acceptance prior to be deployed into production. Test engineers utilize an automated “registration” system that collects information on the component being tested, the business unit it supports and relevant engineering, operations and business owners of the element. The test engineer is then asked a series of questions that identifies the security capabilities of the component in relation to applicable security policies and standards. A security audit is then performed on the component to identify known security exposures. Any gaps identified are then assigned to a security engineer who can proactively work with the test engineer on remediation actions prior to the component being deployed into production.

All systems are audited on a daily basis with audit report details provided to system owners for remediation and to Security Operations (ISSM) for compliance tracking. Security metric data is generated on a monthly basis and formally reviewed by the Operations, Engineering and Architecture organizations. Formal Operations Sciences methodology, with oversight from an Operations Control Office, is used to establish metric targets. Service Improvement Plans (SIPs) are created on all yellow and red metrics to ensure proper tracking of corrective action takes place.

Level 3 utilizes third party audits that target specific technical, organizational and operational controls to identify corrective gaps. Output from the third party audits is implemented into the strategic and tactical roadmaps.