DRAFT

COMMITTEE T1 – TELECOMMUNICATIONS
Working Group T1M1.5 T1M1.5/2003-007R5
May 24, 2003

DOCUMENT TYPE: DRAFT AMERICAN NATIONAL STANDARD

TITLE: **Baseline Security Requirements for the Management Plane**

SOURCE*: **T1M1.5 Security Requirements Ad Hoc Group**

PROJECT: Management Services, TMN

ABSTRACT

This contribution is a revision to T1M1.5/2003-007R4. It captures changes agreed to during the second LB117 default letter ballot. Since the ATIS/T1 Chief Editor will remove and replace any table of contents supplied by the Editor and since the Chief Editor has requested that auto-numbering headers not be used in draft standards, no table of contents is supplied at this time with this draft standard.

NOTICE

This is a draft document and thus, is dynamic in nature. It does not reflect a consensus of Committee T1-Telecommunications and it may be changed or modified. Neither ATIS nor Committee T1 makes any representation or warranty, express or implied, with respect to the sufficiency, accuracy or utility of the information or opinion contained or reflected in the material utilized. ATIS and Committee T1 further expressly advise that any use of or reliance upon the material in question is at your risk and neither ATIS nor Committee T1 shall be liable for any damage or injury, of whatever nature, incurred by any person arising out of any utilization of the material. It is possible that this material will at some future date be included in a copyrighted work by ATIS.

* CONTACT: Tom Grim; E-mail: tgrim@tri.sbc.com; Tel: 512-372-5835; Fax: 512-372-5891

Draft proposed American National Standard

for Telecommunications

Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

Secretariat

Alliance for Telecommunications Industry Solutions

Approved Month__, 20__

American National Standards Institute, Inc.

Abstract

This standard contains a set of baseline security requirements for the management plane. The President's National Security Telecommunications Advisory Committee Network Security Information Exchange (NSIE) and Government NSIE jointly established a Security Requirements Working Group (SRWG) to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. In the telecommunications industry, this access incorporates operation, administration, maintenance, and provisioning for network elements and various supporting systems and databases. Members of the SRWG, from a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. This initial list of security requirements was submitted as a contribution to Committee T1 – Telecommunications, Working Group T1M1.5 for consideration as a standard. The requirements outlined in this document will allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure.

Foreword

The information contained in this foreword is not part of this American National Standard (ANS) and has not been processed in accordance with the American National Standards Institute's requirements for an ANS. As such, the foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the standard.

Executive Orders and Presidential directives and commissions have identified eight infrastructures as critical national assets necessary for the defense and economic security of the United States. Telecommunications is one of these critical infrastructures. The President's National Security Telecommunications Advisory Committee Network Security and Information Exchange (NSIE) and Government NSIE established a Security Requirements Working Group (SRWG) to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. In the telecommunications industry, this access incorporates operation, administration, maintenance, and provisioning for network elements and various supporting systems and databases (i.e., operational support system).

Members of the SRWG, from a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. This initial list of security requirements was submitted as a contribution to Committee T1 – Telecommunications, Working Group T1M1.5 for consideration as a standard.

Although these requirements employ telecommunications terms and formats, the underlying principles should apply equally to the management of computing elements in the other infrastructures. Other infrastructures may wish to modify and apply these recommendations as appropriate to their respective infrastructure.

This document is entitled Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane. There are three annexes in this standard that are informative and are not considered part of this standard. Footnotes are not officially part of this standard.

Future control of this document will reside with Accredited Standards Committee – Telecommunications, T1. This control of additions to the specification, such as protocol evolution, new applications, and operational requirements, will permit compatibility among U.S. networks. Such additions will be incorporated in an orderly manner with due consideration to the International Telecommunication Union – Telecommunications Sector layered model principles, conventions, and functional boundaries.

Suggestions for improvement of this standard are welcome. These should be sent to the Alliance for Telecommunications Industry Solutions, T1 Secretariat, 1200 G Street, NW, Suite 500, Washington, DC 20005.

T1M1.5 Committee members list:

Working Group T1M1.5 – Security Requirements Ad Hoc Group developed this standard. Over the course of its development, the following individuals participated in the group's discussion and made significant contributions to the standard:

Michael McGuire, Chair
Tom Grim, Vice Chair
Stuart Jacobs, Technical Editor
Michael Lee, Technical Editor
Greg Shannon, Technical Editor
Marcia McGowan, Editorial Editor

Andrea Livero-Scott, Editorial Editor

Contributors:

Brennan Baybeck
Bob Beeman
Kathy Blasco
David Dumas
Jack Edwards
Renee Esposito
Mike Fargano
Mike Frank
Richard Graveman
Martin Hogg
Frank Horsfall
George Jones
John Kimmins
Hing-Kam Lam
Christopher Lonvick
Hank Mauldin
Kevin McMahon
Lakshmi Raman
Moshe Rozenblit
Jim Stanco
Fred Staples
Rod Wallace
Joe Wolfkiel
Bob Wright

Table of Contents

Table of Tables

Table of Figures

Draft proposed American National Standard for Telecommunications –

Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

0 Introduction

Executive Orders and Presidential directives and commissions have identified telecommunications as a critical infrastructure, necessary for the defense and economic security of the United States of America. Appropriate security for the network management functions controlling this infrastructure is essential. Many standards for network management security exist. However, compliance is low and implementations are inconsistent across the various telecommunications equipment and software components. This document identifies a minimum set of requirements to allow vendors, Government departments and agencies, and service providers to implement a secure network management infrastructure. Although the present baseline represents the current understanding of the state of the art, technologies will advance and conditions will change. To be successful, this document must evolve as conditions warrant. This document is intended as a foundation. Service providers may include unique requirements to meet specific needs over and above those in this baseline.

1 Scope, Purpose, and Application

In some telecommunications networks, management traffic is often transmitted on a separate network from that carrying the service provider's end-user traffic. In these networks, security threats to the management plane are completely isolated from any malicious activity on the end-user plane. The management plane is relatively easy to secure because access to this plane is restricted to known administrators and traffic is restricted to known management activities. However, in some cases management traffic is combined on a single network with the service provider's end-user traffic. Combining traffic in this manner minimizes costs by requiring only a single integrated network infrastructure; however, many new security challenges are introduced. Threats in the end-user plane now become threats to the management and control planes. The management plane now becomes accessible to the multitude of end-users and many types of malicious activities become possible. The purpose of this document is to recommend minimum baseline security mechanisms to help mitigate security risks in the management of telecommunications networks.

To provide a complete end-to-end solution, all security measures (e.g., access control, authentication) should be applied to each type of network activity (i.e., management plane activity, control plane activity, and end user plane activity) for the network infrastructure, network services, and network applications. This document focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the network infrastructure. As such, the document addresses only one aspect of an overall end-to-end security solution, but may be used as a starting point for subsequent documents addressing the security of “control” and “end user” planes, as appropriate.

The requirements in this standard are applicable to NEs and MSs to be deployed in the future. For NEs in the network that do not meet all the mandatory security requirements, the overall security requirements at the network architecture design should be supported. This document addresses security for NE, MS, and element management system (EMS) equipment, and does not specifically address security for other equipment such as customer premise equipment (e.g., voice over Internet Protocol [IP] telephones) or independent test gear. For such other equipment, all mandatory requirements in this document should be considered objective recommendations.

1.1 Framework and Model

In the context of this document, to secure something means to protect it (i.e., computers, networks, data, or other resources) from unauthorized access, use, or activity. Loss of data, denial of service (DoS), theft of service, and loss of customer confidence are only some of the results of security incidents. System and network administrators need to protect systems and their component elements from users and from attackers. Although security is multifaceted (spanning operations, physical, communications, processing, and personnel), of concern here are security problems resulting from weaknesses inherent in commonly employed configurations and technology. A threat consists of, but is not limited to, disclosure, unauthorized use, change, and denial of service. Table 1 lists some security threats.

Table 1 – Threats

Threat Category*)	Examples of Threats
Unauthorized Access	Hacking Unauthorized system access to carry out attacks Theft of service
Masquerade	Session replay Session hijacking Man-in-the-middle attacks
Threats to System Integrity	Unauthorized manipulation of system configuration files Unauthorized manipulation of system data
Threats to Communication Integrity	Unauthorized manipulation of data in transit
Threats to Confidentiality	Eavesdropping Session recording and disclosure Privacy violations
Denial of Service	Transmission control protocol (TCP) SYN flood[1] Malformed packet attacks Distributed DoS
*) Derived from American National Standards Institute T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning—Security Framework for Telecommunications Management Network Interfaces* and International Organization of Standardization (ISO) 7498-2: 1989 *Information Processing Systems—Open Systems Interconnection Basic Reference Model—Part 2: Security Architecture*.	

These security threats may be minimized or mitigated within a network system or NE platform or application by inclusion of security services (as defined in ISO 7498-2:1989 *Information Processing Systems—Open Systems Interconnection Basic Reference Model—Part 2: Security Architecture*) to enforce the following:

[1] CISCO comment #9 from 3m150041.doc

- Identification and AUTHENTICATION
- Authorization and ACCESS CONTROL Level
- Data Integrity
- Privacy and Confidentiality
- Nonrepudiation.

This document addresses security for the management plane—that is, security features to ensure that the network can be administered and managed in a secure manner. Some vulnerability may still exist, even after following the recommendations contained in this document. The following risks are among those with the capability to compromise the management plane:

- Inappropriate actions by authorized users. These actions can be either malevolent or accidental.
- Security for the control plane (e.g., signaling, routing, naming, and discovery protocols) and the end-user plane.
- The effects of vulnerabilities in specific protocols.
- Malware (e.g., viruses, Trojan horses, worms, or other embedded code). Once malware successfully compromises any NE/MS, the malware may use the secure network communication links to transmit attacks to other NE/MS components. These attacks may continue until network managers detect the attack and take action to eliminate it.

This document is concerned with the security of management traffic, especially when it traverses networks mixed with end-user traffic. Figure 1 illustrates a reference model that is used to specify network management security solutions. This model is used to examine logical communication paths within the entire network and quantify which protocols are used for communications on each path. Using this model, threats and vulnerabilities can be examined for each path, and appropriate security mechanisms can be applied.

Multivendor NEs are shown at the bottom of the model in figure 1. EMSs that provide specific management functions for the particular NE are illustrated above the NE. The network management system (NMS) itself is at the top of the model. The NMS provides overall management to the NE and EMS, and contains the specific service management applications and the business management applications, such as configuration and billing systems. Remote and local operators are also shown in the model and communication paths are shown with all other system elements.

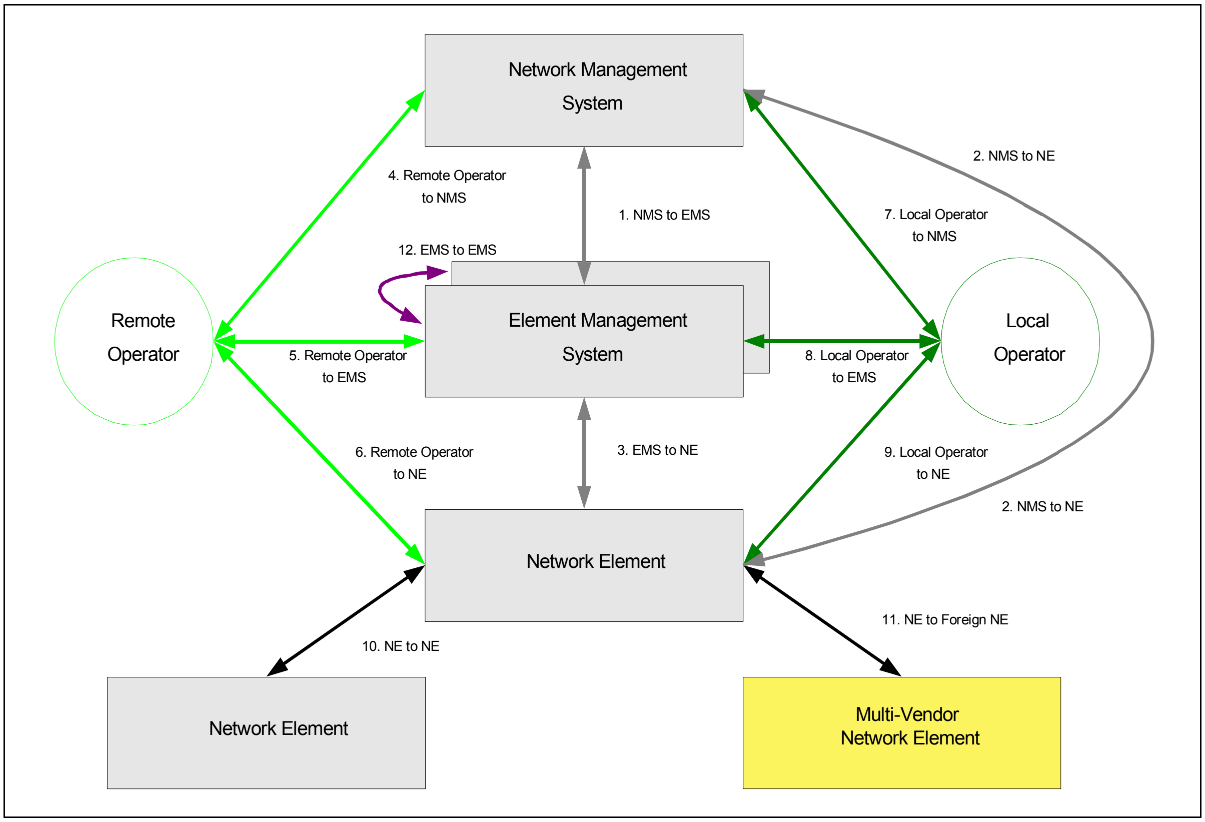

Figure 1 – Network management security reference model

The Security Reference Model (figure 1) may also be useful in correlating telecommunications management network (TMN)-defined interfaces to the security model. The TMN is defined in International Telecommunication Union – Telecommunications Sector (ITU-T) Recommendation M.3010, *Principles for a telecommunications management network*. It is defined as an architecture for management, including planning, provisioning, installation, maintenance, operations, and administration of telecommunications equipment, networks, and services.

In the TMN standard, against which service providers have indicated they will standardize, it is identified that multiple network infrastructures and multiple TMNs may exist. In fact, the management of NEs by their associated MSs in the typical service provider environment may traverse numerous data communications networks (DCN). This management traffic may need to negotiate several access control mechanisms (e.g., firewall devices or router access lists, and/or network connections and interconnections) in order to get to the NE in question. NEs must traverse many of the same networks and interconnections for return traffic. As such, vendors should know and understand the possible latency issues and work towards delivering solutions to address those issues.

1.2 Design Guidelines

Table 2 presents design guideline objectives that attempt to satisfy the requirements in clause 5 to mitigate the threats proposed in Table 1.

Table 2 – Design Guidelines Considered

Guideline	Description
Isolation	Insulation of management traffic from customer traffic

Guideline	Description
Effective Security Policies	Requirements and supporting architectures must allow for policies that are definable, flexible, enforceable, auditable, verifiable, reliable, and usable
Strong AUTHENTICATION, Authorization, and Accounting (AAA)	Two-factor and cryptographically secure AAA
Highest Benefit for a Given Cost	Improve security by implementing security mechanisms that have widely available implementations and wide spread deployment, so that use histories allow security mechanisms to be reviewed
Path for Improvement	Consider next steps for enhancing and improving network management security to further satisfy given requirements with evolving technology and mechanisms or to satisfy newly defined security requirements
Technical Feasibility	Requirements must be satisfied with products, solutions, and/or technologies available today
Housekeeping	Requirements should be consistent with standard operating procedures of well-run network management operations
Open Standards	Use ideas and concepts that are already standardized (e.g., IP security [IPsec], digital signatures). All aspects of the open standards should be addressed including system, protocols, modes, algorithm, option, key size, and encoding

1.3 Applicability of this document to the TMN

This document applies to the entirety of the TMN covering both circuit-based NEs and packet-based NEs. Circuit-based NEs provide multiple logical interfaces between switches, transmission elements, signaling elements, and other special-purpose elements that are designed and developed to support traditional telephony services. The packet-based NE model has migrated from the centralized system where all functions were hosted on one platform to a more distributed system where functions may be hosted by multiple platforms coupled together to form a complete system. These functions can be service or operations related. This document provides a security framework to protect all of the facilities of the NE/MS that are exposed to various threats and risks. This includes platforms, visible interfaces, and associated functions, applications, and services. To provide equal protection to all types of NE/MS, the total overall system security features should be the same for all types of NE/MS. However, depending on the architecture of the resident and distributed features and the available processing capabilities, the implementation scheme of the security features in NE/MS may be different in its details.

Some NE/MS will have the capacity to incorporate security features within themselves. They can fully implement all of the mandatory security requirements in this document. Other NE/MS will not have the capacity to incorporate all of the mandatory security features defined in this document within them. It may be unrealistic to ask for all security features to be embedded within the NE/MS operating system (OS) or application layers of these devices. For these types of devices that exist in or are placed into a network their security properties should be augmented so that the system meets the requirements of this standard. As an example, if a MS cannot provide STRONG ENCRYPTION for MANAGEMENT ACTIONS over a TRUSTED PATH, then an auxiliary device may be placed in the network path so that MANAGEMENT COMMUNICATIONS passing through this device may be performed over an encrypted SESSION. As another example, if an NE cannot directly enforce COMPLEX PASSWORDS, then it may utilize an ACCESS CONTROL server (ACS) that can.

2 Normative References

The following standards contain provisions, which, through reference in this text, constitute provisions of this American National Standard (ANS). At the time of publication, the edition indicated was valid. All standards are subject to revision, and the parties to agreements based on this ANS are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below.

ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation.* (available from the ANSI X9 Electronic Standards Store, http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80)

ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* (available from the ANSI X9 Electronic Standards Store, http://webstore.ansi.org/ansidocstore/dept.asp?dept_id=80)

Federal Information Processing Standards (FIPS) Publication 46-3, *Data Encryption Standard*, National Institute of Standards and Technology, October 1999, (available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)

FIPS Publication 81, *Data Encryption Standard Modes of Operation*, National Institute of Standards and Technology, December 1980, (available at http://www.itl.nist.gov/fipspubs/fip81.htm)

FIPS Publication 180-1, *Secure Hash Standard*, National Institute of Standards and Technology, April 1995, (available at http://www.itl.nist.gov/fipspubs/fip180-1.htm)

FIPS Publication 186-2, *Data Signature Standard*, National Institute of Standards and Technology, January 2000.

FIPS Publication 197, *Advanced Encryption Standard*, National Institute of Standards and Technology, November 2001, (available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

Internet Engineering Task Force (IETF) Request for Comment (RFC) 1321. *The MD5 Message-Digest Algorithm*. R. Rivest, April 1992, (available at http://www.ietf.org/rfc/rfc1321.txt?number=1321)

IETF RFC 1750. *Randomness Recommendations for Security.* D. Eastlake, S. Crocker, and J. Schiller, December 1994, (available at http://www.ietf.org/rfc/rfc1750.txt?number=1750)

IETF RFC 2104. *Hashed Message Authentication Code: Keyed-Hashing for Message Authentication.* H. Krawczyk, M. Bellare, and R. Canetti. February 1997.

IETF RFC 2403. *The Use of Hashed Message Authentication Code with Message Digest 5-96 within the Encapsulating Security Payload and the Authentication Header*. C. Madson, R. Glenn, November 1998, (available at http://www.ietf.org/rfc/rfc2403.txt?number=2403)

IETF RFC 2404. *The Use of Hashed Message Authentication Code with Secure Hash Algorithm 1-96 within the Encapsulating Security Payload and the Authentication Header*. C. Madson, R. Glenn, November 1998, (available at http://www.ietf.org/rfc/rfc2404.txt?number=2404)

IETF RFC 2409, *The Internet Key Exchange [IKE]*. D. Harkins and D. Carrel. November 1998 (available at http://www.ietf.org/rfc/rfc2409.txt?number=2409)

IETF RFC 2437. *PKCS #1: Rivest, Shamir, and Adleman Cryptography Specifications Version 2.0*. B. Kaliski, J. Staddon. October 1998, (available at http://www.ietf.org/rfc/rfc2437.txt?number=2437)

IETF RFC 2459. *Internet Public Key Infrastructure: Part I: X.509 Certificate and Certificate Revocation List Profile*. Housley, R., W. Ford, W. Polk, and D. Solo, January 1999, (available at http://www.ietf.org/rfc/rfc2459.txt?number=2459).

IETF RFC 2945. *The SRP Authentication and Key Exchange System*. T. Wu. September 2000, (available at http://www.ietf.org/rfc/rfc2945.txt?number=2945).

IETF RFC 1305. *Authentication Issues, Appendix C.* D. Mills. March 1992, (available at http://www.ietf.org/rfc/rfc1305.txt?number=1305).

ITU-T Recommendation G.8080/Y.1304. *Architecture for the Automatically Switched Optical Network (ASON).* November 2001, (available at ITU Electronic Bookshop)

ITU-T Recommendation X.500. *The Directory: Overview of Concepts, Models and Service*, (available at ITU Electronic Bookshop)

ITU-T Recommendation X.509. *Information Technology - Open Systems Interconnection: The Directory: Authentication Framework*, August 1997, (available at ITU Electronic Bookshop)

National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001 (available at http://cs-www.ncsl.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf)

3 Definitions

The following terms appear in capital letters when they are used in a requirement statement.

3.1 Access Control: The prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner.[2]

3.2 Application Administrator: A role responsible for the proper activation, maintenance, and usage of an NE/MS application. Application administration tasks include upgrading application software.[3]

3.3 Application Security Administrator: A role responsible for the proper activation, maintenance, and usage of the application layer security features of a NE/MS. Represents the highest level of security authority for a NE/MS application instance. Tasks include:

- Define and assign new user and group privileges at the application level
- Maintain a record of all requests for login IDs to the application
- Add and delete users at the application level
- Monitor all application security logs
- Configure application security logging and alarms
- Manage application security logging processes

[2] Taken from ANSI T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning—Security Framework for Telecommunications Management Network Interfaces*, Clause 3.1.

[3] This task may be a function of the SYSTEM ADMINISTRATOR, if SUPERUSER authority is necessary to complete this task. Processes may be developed to control access to the SUPERUSER account.

- Terminate any user application session

3.4 Application User/Operator: A role that has authorization to access business and management functions provided by the NE/MS but has no authorization to access any system administration or security administration operations within a system other than changing one's own password.

3.5 Authentication: AUTHENTICATION is the act of verifying a claimed identity.

3.6 Complex Passwords: A password is characterized as "complex" when it has some combination of alphabetic, numeric, and special characters.

3.7 Control Plane: The CONTROL PLANE performs call control and connection control functions. Through signaling, the CONTROL PLANE sets up and releases connections, and may restore a connection in case of a failure.[4]

3.8 Critical Security Administration Actions: A SYSTEM SECURITY ADMINISTRATOR is responsible for the proper activation, maintenance, and usage of the security features of a system (NE/MS). CRITICAL SECURITY ADMINISTRATION ACTIONS include, but not limited to:

- Define and assign user privileges
- Add and delete user IDs
- Disable the use of specific user IDs as login IDs
- Initialize and reset login passwords
- Initialize and change cryptographic keys
- Set the system's aging threshold for login passwords
- Set the system's limit on the number of failed logins for each login ID
- Remove a lockout, or change the system's lockout timer value
- Set the system's inactivity timer value
- Set system security logging and alarm configuration
- Manage the security logging processes
- Upgrade security software
- Terminate any user or system session

3.9 Disable/Disabled: When referring to a user ID, a state in which the user ID cannot be used for login until the ID has been enabled by specific action from another user ID with the appropriate authorization privileges (e.g. SYSTEM SECURITY ADMINISTRATOR or APPLICATION SECURITY ADMINISTRATOR).

[4] ITU-T Recommendation G.8080/Y.1304. *Architecture for the Automatically Switched Optical Network*, November 2001, (available at ITU Electronic Bookshop)

3.10 Key Strength: Different cryptographic algorithms have varying degrees of security depending on how difficult they are to break. A cryptographic algorithm is considered strong if it is computationally infeasible to break—that is, it has sufficient complexity that it cannot be broken with available resources either currently or in the foreseeable future. Computational complexity is most often measured in terms of processing complexity, or the amount of time and memory space needed to perform an attack. Although the complexity of an attack remains constant for a particular algorithm and key size, computing power is constantly increasing. Good cryptosystems are designed to be infeasible to break with the computing power that is expected to evolve many years in the future. As a result of the rapid development of new technology and cryptanalytic methods, the correct key size for a particular application is continuously changing.

3.11 Lockout/Locked Out: When referring to a user ID, a state in which the user ID cannot be used for login until the lockout state has been removed by one or more appropriate actions. Appropriate actions include, but are not limited to:

- Automatic reset after a threshold period of time has elapsed (e.g., after 60 minutes),

- Automatic reset after successful completion of a predefined reset process (e.g., after the owner correctly answers a scripted set of questions), or

- Reset by specific action from another user ID with the appropriate authorization privileges (e.g. SYSTEM SECURITY ADMINISTRATOR or APPLICATION SECURITY ADMINISTRATOR).

3.12 Management Action: Actions undertaken by or on behalf of the SYSTEM ADMINISTRATOR.

3.13 Management Communication: Any communication of a MANAGEMENT ACTION.

3.14 Management Plane: The MANAGEMENT PLANE performs management functions for the TRANSPORT PLANE, the CONTROL PLANE, and the system as a whole. It also provides coordination between all the planes. Performance, fault, configuration, accounting, and security management functional areas identified in ITU-T Recommendation M.3010, *Principles for a Telecommunications Management Network* are performed in the MANAGEMENT PLANE.[5]

3.15 Network Element/Management System: A collective term used to describe the entirety of elements within a telecommunications network including NEs, EMSs, NMSs, and OSSs.

3.16 Network System: Encompasses embedded software and databases including adjuncts, intelligence peripherals, and EMSs. May perform a wide range of functions related to the NE environment.

3.17 Protected Authentication: Includes STRONG AUTHENTICATION, TWO-FACTOR AUTHENTICATION, TRUSTED PATH AUTHENTICATION, cryptographic third-party authentication (e.g., Kerberos), or one-time passwords.

3.18 Session: A sequence of operations, either machine-to-machine or human-to-machine, that are associated with a unique process or user ID.

[5] The TMN architecture is described in ITU-T Recommendation M.3010, *Principles for a Telecommunication Management Network* and additional details regarding the MANAGEMENT PLANE are provided in the M series recommendations. ITU-T Recommendation G.8080/Y.1304, *Architecture for the Automatically Switched Optical Network*, November 2001 (available at ITU Electronic Bookshop)

3.19 Strong Authentication: AUTHENTICATION that relies on the use of cryptographic techniques (e.g., public key encryption, symmetric key encryption, digital signatures, digital hashing techniques).[6] STRONG AUTHENTICATION should include two-way authentication, which can be used to prevent active attacks.

3.20 Strong Encryption: A brute force attack occurs when an attacker tries all possible key combinations using available computing resources. In this fashion, the correct key can be found on average after one-half of all possible key combinations have been tried. The expected time to test one half of the key combinations is a measure of the strength of the encryption. Therefore, at any given time, STRONG ENCRYPTION mechanisms use algorithms and keys such that it would take any attacker more than 2 years to break.

3.21 SuperUser: A role, which has complete access to all resources within a system and the applications residing on that system (e.g. "root" for UNIX systems). SUPERUSER roles can be used during installation, but should be used only in emergency situations for operational systems.

3.22 System Administrator: A role responsible for OS level processes and procedures pertaining to installation, operations, and maintenance of the operating platform; installation of software on the platform; and control of SUPERUSER authority. Tasks include:

- Coordinate the installation of a new platform
- Define and assign new user and group privileges at the OS level
- Maintain a record of all requests for login IDs to the OS
- Add and delete users at the OS level
- Disable the use of specific IDs as login IDs (bin, sys, uucp)
- Install OS upgrades and patches
- Install application and database software to the OS
- Monitor all system logs
- Maintain and monitor access and changes to SUPERUSER password
- Control access to the SUPERUSER account, allowing appropriate access as the business requires
- Manage system logging processes
- Delegate administration authorizations to specific persons in other roles, including APPLICATION ADMINISTRATORS
- Terminate any user or system session

[6] American National Standards Institute T1.243-1995, *Operations, Administration, Maintenance, and Provisioning—Baseline Security Requirements for the Telecommunications Management Network*. Also refer to International Organization of Standards/International Electrotechnical Commission 9594-8, *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*, 1998 (available at International Organization of Standards Online Store)

3.23 System Security Administrator: A role that is responsible for the proper activation, maintenance, and usage of the system security features of a NE/MS. Represents the highest level of security authority for a system/application instance. Tasks include:

- Define and assign new user and group privileges at the OS level
- Maintain a record of all requests for login IDs to the OS
- Add and delete users at the OS level
- Disable the use of specific IDs as login IDs (bin, sys, uucp)
- Monitor all system security logs
- Initialize and change cryptographic keys
- Set the system's aging threshold for login passwords
- Set the system's limit on the number of failed logins for each login ID
- Remove a lockout or changing the system's lockout timer value
- Set the system's inactivity timer value
- Configure system logging and alarms
- Manage system security logging processes
- Delegate security authorizations to specific persons in other roles, including APPLICATION SECURITY ADMINISTRATORS
- Terminate any user or system session

3.24 Transport Plane: The TRANSPORT PLANE provides bi-directional or unidirectional transfer of user information from one location to another. It can also provide transfer of some control and network management information. The TRANSPORT PLANE is layered; it is equivalent to the transport network defined in ITU-T Recommendation G.8080/Y.1304, *Architecture for the Automatically Switched Optical Network*.[7]

3.25 Trusted Path: A mechanism by which any user/operator-to-system or system-to-system interactions with a system are secured. This mechanism can be activated only by the user/operator or system and cannot be imitated. A TRUSTED PATH can either be a dedicated physical path (i.e., a terminal directly connected to the system) or an encrypted pathway, which includes integrity and replay protection (e.g., "secured" virtual private network, Secure Socket Layer [SSL] tunnel, Secure Shell [SSH]).[8]

[7] ITU-T Recommendation G.8080/Y.1304, *Architecture for the Automatically Switched Optical Network,* November 2001 (available at ITU Electronic Bookshop).

[8] Adapted from National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*, October 1998 (available at http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

3.26 Two-Factor Authentication: TWO-FACTOR AUTHENTICATION is a commonly used term to describe an AUTHENTICATION process that requires two components: possession of a physical entity (e.g., token or card), and knowledge of a secret (e.g., password or passphrase).

4 Abbreviations

AAA	Authentication, Authorization, and Accounting
ACS	Access Control Server
AES	Advanced Encryption Standard
ALE	Annualized Loss Expectancy
ANS	American National Standard
ANSI	American National Standards Institute
CALEA	Communications Assistance for Law Enforcement Act
CO	Central Office
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CSI	Common Secure Interoperability
DCN	Data Communication Network
DES	Data Encryption Standard
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EMS	Element Management System
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HAZMAT	Hazardous Materials
HMAC-MD5-96	Hashed Message Authentication Code with Message Digest 5
HMAC-SHA-1-96	Hashed Message Authentication Code with Secure Hash Algorithm 1
HTTP	Hypertext Transfer Protocol

IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU-T	International Telecommunication Union – Telecommunications Sector
LAES	Lawfully Authorized Electronic Surveillance
MS	Management System; any EMS, NMS, or OSS[9]
NE	Network Element
NE/MS	NE or MS
NIST	National Institute of Standards and Technology
NMS	Network Management System
OAM&P	Operations, Administration, Maintenance and Provisioning
OASIS	Organization for the Advancement of Structured Information Standards
OEM	Original Equipment Manufacturer
ORB	Object Request Broker
OS	Operating System
OSI	Open Systems Interconnect
OSS	Operations Support System
PPP	Point-to-Point Protocol
RFC	Request for Comment
RMAC	Randomized Message Authentication Code
RSA	Rivest, Shamir, and Adleman
SAML	Security Assertion Markup Language

[9] OSSs generally can be used in the same context as MSs on any layer of the telecommunications management network hierarchy.

SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
TLS	Transport Layer Security
TMN	Telecommunications Management Network
TRA	Telecommunications Reform Act
UDP	User Datagram Protocol
XML	Extensible Markup Language

5 Security Requirements

This clause contains the specific baseline requirements for operations, administration, maintenance, and provisioning (OAM&P) and operations support system (OSS) security as they specifically apply to MANAGEMENT PLANE security for infrastructure, services, and applications.

This clause addresses six essential principles of OAM&P security:

- Secure management traffic with STRONG ENCRYPTION and AUTHENTICATION
- Authenticate and attribute all MANAGEMENT ACTIONS
- Manage security resources and configurations with integrity
- Maintain logs for all of the above
- Support least privilege
- Support security alarms

  NOTE – Security alarms are an area for further study.

The following table outlines the organization of this clause.

Clause	Contents
Clause 5.1	Discusses required security (cryptographic) algorithms and lays out key length and key management requirements
Clause 5.2	Discusses requirements for AUTHENTICATION
Clause 5.3	Discusses requirements for administration

Clause 5.4	Describes specific security requirements for the management of NE/MS
Clause 5.5	Lays out requirements for OAM&P communications (i.e., physical or virtual management of communications networks, also known as DCN in some companies)
Clause 5.6	Discusses requirements for NE/MS development and delivery

All requirements outlined in this clause that have a prefix of M-xxx are mandatory and must be met by available components. All requirements that have a prefix of O-xxx are considered to be objectives. Objective requirements need additional examination; however, it is likely that in the future, industry will coalesce around them and develop standards to address the requirements.

5.1 Cryptographic Algorithms and Keys

This clause specifies requirements for cryptographic algorithms, key lengths, and key management to help ensure system and network security. Symmetric algorithms are normally used for both confidentiality and integrity services. The keys for symmetric algorithms should normally be exchanged in a process tightly bound to authentication, lest an attacker get between the authentication and key distribution processes. Asymmetric algorithms can also be used in support of authentication and key exchange services. The methods used to generate, store, distribute, destroy, and revoke these keys are of paramount importance. In addition, factors such as key length, key selection, and algorithm selection have a direct bearing on the amount of security a cryptosystem provides. Key lengths recommended in this clause are appropriate at present; however, increases in key lengths will be required in the future. Cryptographic algorithms may need to be updated in the future to ensure STRONG ENCRYPTION will be provided.

PROTECTED AUTHENTICATION and data confidentiality can be based on a cryptographic foundation. Cryptography uses special algorithms that are and should be standards-based and publicly available thereby allowing for widespread scrutiny and ease of implementation. The “strength” of this concept is in the keys (i.e., strength refers to the amount of time required to reverse engineer [i.e., find or guess] the key value(s) being used with a specific algorithm).

Security protocols (e.g., IPsec, SSL, SSH) typically provide AUTHENTICATION, integrity, and confidentiality. Security extensions to other protocols such as Simple Network Management Protocol Version 3 [SNMPv3][10], Common Object Request Broker Architecture [CORBA], Border Gateway Protocol, and Open Shortest Path First are designed to provide AUTHENTICATION and integrity. PROTECTED AUTHENTICATION and integrity are essential between NE/MS and, where deemed appropriate, confidentiality is also required.

5.1.1 Symmetric Encryption Algorithms

Symmetric, or secret key encryption, refers to a cryptographic system where enciphering and deciphering keys are the same. Symmetric cryptosystems require that initial arrangements be made for the individuals to share a unique secret key. The key must be distributed to the individuals via a secure means, because knowledge of the enciphering key implies knowledge of the deciphering key and vice-versa.

For symmetric encryption, 128-bit Advanced Encryption Standard (AES) should be used. AES with greater than 128-bit key length (i.e., 192- or 256-bit key AES) may also be used. Fifty-six (56)-bit Data Encryption Standard (DES) has keys that are considered to be too short to be effective and should not be used for any purpose unless required for export. Three key triple data encryption algorithm (TDEA)[11] is

[10] SNMPv3 may also provide confidentiality.

[11] TDEA is specified in Federal Information Processing Standard (FIPS) Publication 46-3, *Data Encryption Standard*, October 1999, Appendix 2, Page 22 (available at http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)

acceptable but is not recommended if AES is available. Key length may not be indicative of actual key strength.[12] For clarity, this information is presented in tabular format in Table 3. Other considerations that impact the level of security for encryption including the mode of operation, initialization vector, rekeying intervals, padding, and integrity checks also need to be addressed to provide robust confidentiality. These considerations are outside the scope of this document; however, they are addressed in references cited in clause 2 and annex C.

M-1. For all symmetric encryption applications, algorithms with strengths similar to AES or TDEA shall be used. DES may be used where law prohibits longer algorithms.

5.1.2 Asymmetric Encryption Algorithms

An asymmetric encryption system is one in which the enciphering and deciphering keys are related but different. One is made public, whereas the other is kept secret. The public key is different from the private key, and no feasible way is known for deriving the private key from the public key. Public keys are distributed widely; however, the private key is always kept secret. The use of asymmetric encryption is usually limited to the encryption of symmetric keys for key exchange and the signing of message digests for digital signatures. In key exchange, the recipient's public key is used and in the signing of message digests the signer's private key is used.

For asymmetric encryption, the Rivest, Shamir, Adleman (RSA) algorithm is recommended to be used with a key length of 2,048 bits or greater, which is roughly equivalent in cryptographic strength to the 128-bit symmetric key encryption. The Diffie-Hellman key agreement algorithm with a prime group of 2,048 bits or greater may also be used (e.g., as employed in the IKE protocol). Elliptic Curve Cryptography (ECC) is a new method of performing public key cryptography (i.e., comparable to the RSA algorithm). With ECC, an elliptic curve is defined over a certain field; then, the elliptic curve discrete logarithm problem is solved over this field. The main advantage of ECC as compared to other public-key algorithms is the key size. A 160-bit ECC key is approximately equivalent in security to a 1,024-bit RSA algorithm key, and a 210-bit ECC key is approximately equivalent to a 2,048-bit RSA algorithm. The smaller ECC key results in less computational overhead and a more efficient cryptosystem.[13] For clarity, this information is presented in tabular format in Table 3. Issues such as formatting, padding, handling error conditions, and choosing appropriate primes and the size of the public exponent, and in the case of ECC, base field and curve must also be considered; however, these issues are outside the scope of this document. References in clause 2 and annex C address them in detail.

M-2. For all asymmetric encryption applications, algorithms with strengths similar to the RSA 2,048-bit key algorithm shall be used.

M-3. For all key exchange applications, algorithms with strengths similar to 2,048-bit RSA or Diffie-Hellman algorithms with a prime group of 2,048 bits shall be used.

5.1.3 Data Integrity Algorithms

Keyed message digest algorithms combined with hashing functions are used to ensure data integrity for arbitrary length messages. For symmetric data integrity where the sender and receiver have the same key, the Hashed Message Authentication Code with Message Digest 5 (HMAC-MD5-96)[14] algorithm or

[12] TDEA can be performed using either two independent 56-bit keys or three independent 56-bit keys, which could be expected to have a strength of 112 bits and 168 bits, respectively. However, TDEA is subject to the "meet in the middle" attack, which can reduce two key 3DES strength to only 57 bits rather than the expected 112 bits. The same attack can render three key TDEA strength to only 112 bits rather than the expected 168 bits. Thus, TDEA should be used with three independent keys and the worst case strength should be assumed to be 112 bits. Source: Bruce Schneier, *Applied Cryptography*, Second Edition, 1996, John Wiley & Sons, Chapter 15.2, p. 358.

[13] See *Digital Signature Standard*, November 2002, (available at http://csrc.nist.gov/cryptval/dss.htm) for additional details on RSA, Diffie-Hellman, and ECC algorithms.

[14] Internet Engineering Task Force Request for Comment 2403, *The Use of HMAC-MD5-96 within ESP and AH*, C. Madson, R. Glenn, November 1998.

the Hashed Message Authentication Code with Secure Hash Algorithm 1 (HMAC-SHA-1-96)[15] algorithm is acceptable.

M-4. For all symmetric secure data integrity applications, algorithms with strengths similar to HMAC-MD5-96 with 128-bit keys, HMAC-SHA-1-96 with 160-bit keys, or AES-based randomized message authentication code (RMAC) shall be used.

The Digital Signature Algorithm (DSA), with a key length of 1,024 bits or greater in length, and the RSA algorithm are standards for asymmetric data integrity where public-private key pairs are used.

M-5. For all asymmetric secure data integrity applications, an algorithm at least as strong as DSA or the RSA algorithm shall be used.

5.1.4 Keys for Cryptographic Algorithms

According to current best practices for KEY STRENGTH, when a key is chosen, it should be expected that it can not be broken by any attacker in less than 2 years. The key length recommendations in this clause are made with this in mind.

M-6. Any key for encryption or data integrity shall have a KEY STRENGTH that takes any attacker at least 2 years to break using known technology when first provided or used. Weaker keys may be used only when stronger encryption is prohibited by law.

Table 3 – Cryptographic Algorithm Requirements

Category	Algorithm	Minimum Key Length as of October 2002	Optional Key Lengths	Comments
Symmetric Encryption	AES	128 bits	192 bits, 256 bits	Standard algorithm chosen by the National Institute of Standards and Technology (NIST) to replace DES
	TDEA (3 key)	168 bits	N/A	AES preferred
	DES	Not allowed	Not allowed	May only be used when stronger encryption is prohibited by law
Asymmetric Encryption (for key exchange)	RSA	2,048 bits	>2,048 bits	2,048 bits chosen to be roughly equivalent in cryptographic strength to 128 bit symmetric; 1,536 bits is the minimum required so that the key can not be broken by any attacker in less than 2 years
	Elliptic Curve	210 bits	>210 bits	A set of relatively new algorithms. 210 bits chosen to be roughly equivalent in cryptographic strength to 128-bit symmetric

[15] Internet Engineering Task Force Request for Comment 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*, C. Madson, R. Glenn, November 1998.

Category	Algorithm	Minimum Key Length as of October 2002	Optional Key Lengths	Comments
	Diffie-Hellman (for key agreement)	2,048-bit mod *p* [**)] group, 256 bit exponent	>2,048-bit mod *p* group, >256 bit exponent	2,048 bits chosen to be roughly equivalent in cryptographic strength to 128-bit symmetric
Message Verification	DSA (Asymmetric)	1,024 bits	>1,024 bits	1,024 bits mandated by NIST[***)]
	HMAC-MD5-96 (Symmetric)	128 bits	N/A	Hashed message authentication code with message digest 5
	HMAC-SHA-1-96 (Symmetric)	160 bits	N/A	Hashed message authentication code with secure hash algorithm 1

[**)] Mod *p* stands for modulo *p*

[***)] FIPS 186-2 *Digital Signature Standard*, January 2000, Clause 2

5.1.5 Cryptographic Key Management

Properly managing cryptographic key material is difficult and often complex. IETF RFC 1750, *Randomness Recommendations for Security*, provides additional guidance. Below are a few requirements that any effective key management system must satisfy. However, the requirements do not assure the security of the key management system, method, or process.

Secure methods, at a minimum, include not sending keys over a communication medium in the clear and not storing keys in the clear in persistent system memory or storage media. These requirements apply to symmetric encryption keys, message authentication code keys, and asymmetric private keys.

M-7. The NE/MS supplier shall provide capabilities for secure key generation, distribution, storage, and replacement/recovery, as defined in ITU-T Recommendations X.500 and X.509.

M-8. Keys used for symmetric encryption and symmetrically based digital signatures shall be distributed out of band or by secure cryptographic processes.

5.2 Authentication

AUTHENTICATION has two purposes in securing the MANAGEMENT PLANE: (1) it ensures the identity of communications parties, which provides a basis for setting up private communications with full data integrity between two systems; and (2) it provides a basic mechanism for logging and auditing the management activities on any system.

5.2.1 System-to-System Process Authentication

Process AUTHENTICATION provides AUTHENTICATION during data communications between systems (e.g., system-to-system, application-to-application), and is the basis for setting up private communications with full data integrity. During data communications, AUTHENTICATION of the sending entity allows the receiver of a message to ascertain the origin of the message. Within a secure communication channel, cryptographic AUTHENTICATION should be associated with each message to bind the sending entity's identity to the message. The receiver will check the cryptographic information supplied with the message to verify the true identity of the sending entity.

M-9. System-to-system process AUTHENTICATION for communications shall use certificate-based AUTHENTICATION or PROTECTED AUTHENTICATION.

M-10. Certificate-based AUTHENTICATION shall be X.509-based certificate systems.

M-11. STRONG AUTHENTICATION exchanges between systems shall be protected in compliance with M-6.

5.2.2 User Authentication, Passwords, and User IDs

User AUTHENTICATION concerns the AUTHENTICATION of clients involved in the management of the network. In this case, AUTHENTICATION involves proving the true identity of the legitimate user and preventing masquerading by illegitimate imposters. With proper AUTHENTICATION, it is possible to track activities and restrict users to pre-authorized activities or roles as discussed in clause 5.3.

The minimum requirements for AUTHENTICATION are the use of a user ID and static COMPLEX PASSWORD. Other mechanisms may be used as long as the administrators of the NE/MS are confident that the security level is at least as great as that provide by a user ID and static COMPLEX PASSWORD. Other mechanisms that may be considered include:

- A user ID and TWO-FACTOR AUTHENTICATION using a one-time password generator,[16] and
- TWO-FACTOR AUTHENTICATION using a smart-card with credentials stored on it in a protected manner.

M-12. Client AUTHENTICATION for logging in, logging, and auditing on each NE/MS shall be at least as strong as a user ID with a COMPLEX PASSWORD over a previously established TRUSTED PATH.

M-12 presents the baseline security requirement. It is expected that AUTHENTICATION techniques and single sign-on technologies will continue to improve.

O-1 represents an objective requirement that anticipates standardization around single sign-on and digital certificates.

O-1. Client AUTHENTICATION should support methods for secure single sign-on and X.509 public key infrastructure.

In secure single sign-on, the protocol still challenges the entity(s) for credentials; however, a user may not have to enter the credentials because they are securely cached in some way (e.g., Kerberos).

The following requirements help maintain password complexity and are useful for auditing and logging.

M-13. Each NE/MS shall automatically enforce COMPLEX PASSWORDS.

M-14. Minimum complexity rules for COMPLEX PASSWORDS shall be as follows:

- Passwords must be a minimum of eight characters long.
- Passwords must not be a repeat or the reverse of the associated user ID.
- Passwords must be no more than three of the same characters used consecutively.

[16] This clause does not discuss dynamic passwords as those are considered to be outside of the scope of this document.

- Passwords must contain at least three of the following combinations:
    - Alpha characters – at least one lower case alpha character
    - Alpha characters – at least one upper case alpha character
    - Numeric characters – at least one numeric character
    - Special characters – at least one special character

M-15. The NE/MS shall require the entry of the old password to prevent another user from changing a logged-on user's password without their knowledge.

M-16. Each NE/MS shall automatically ensure that each new login password differs from the previous password. The degree of difference shall be configurable, with a default difference in at least two character positions.

Because passwords are typically stored via one-way encryption, the entry of the old password is also required to allow the NE/MS to determine the degree of difference between the old and new passwords.

M-17. Each NE/MS shall support a password history to prevent password reuse. The parameters shall be configurable with a default of at least the past five password iterations and at least 180 days.

M-18. Each user ID shall have its own settable login password.

M-19. Passwords shall be user changeable at the user's discretion, following a configurable minimum interval since the last change. The default shall be one day.

M-20. Each NE/MS shall identify at least one, and not more than two, specific SYSTEM SECURITY ADMINISTRATOR accounts that cannot be LOCKED OUT due to password aging.

A common implementation of M-20 allows the SYSTEM SECURITY ADMINISTRATOR to login from the console with no restrictions on the number of failed logins. Alternatively, that user can have a retry timer (e.g., 60 minutes). If no retry timer is used for non-console attempts, then the password for that user ID is vulnerable to a brute force password attack.

M-21. Each NE/MS shall identify at least one, and not more than two, specific SYSTEM SECURITY ADMINISTRATOR account(s) that cannot be LOCKED OUT due to login failures.

M-22. Each NE/MS shall store user IDs in a nonvolatile manner.

M-23. Each NE/MS shall store login passwords in a nonvolatile and one-way encrypted manner. As an exception to one-way encryption, symmetrically encrypted passwords may be used for passwords that need to be decrypted for internal, transient use in trusted system-to-system communication or single sign-on.[17]

5.3 Administration

Each NE/MS must support the concept of "least privilege" (i.e., a person will have a role and will have authorization to view data, modify data, or initiate MANAGEMENT ACTIONS only for those functions

[17] See clause 5.1 for a discussion of symmetric encryption.

allowed by that role). This clause defines basic requirements for implementing “least privilege” through good system security administration.

5.3.1 Security Administration

Each NE/MS must ensure that only authorized users are allowed to manage system security resources. All administrative actions are linked to specific individuals. Though only five types of users are discussed, many other types of users with varying degrees of privileges may exist, especially with respect to critical security MANAGEMENT ACTIONS. The goal is to ensure that only authorized, privileged users can manage critical security resources.

M-24. Each NE/MS shall have at least five types of user roles: a SYSTEM SECURITY ADMINISTRATOR, an APPLICATION SECURITY ADMINISTRATOR, a SYSTEM ADMINISTRATOR, an APPLICATION ADMINISTRATOR, and an APPLICATION USER/OPERATOR. In the case of embedded systems without a separation of system and application, the NE shall support at least three types of user roles: a combined SYSTEM SECURITY ADMINISTRATOR and APPLICATION SECURITY ADMINISTRATOR, a combined SYSTEM ADMINISTRATOR and APPLICATION ADMINISTRATOR, and an APPLICATION USER/OPERATOR.

M-25. The default user type on each NE/MS shall be the APPLICATION USER/OPERATOR.

M-26. Each NE/MS shall support the following CRITICAL SECURITY ADMINISTRATION ACTIONS:

- Define and assign user privileges.
- Add and delete user IDs.
- DISABLE/enable the use of specific user IDs as login IDs.
- Initialize and reset login passwords.
- Initialize and change cryptographic keys.
- Set the system’s aging threshold for login passwords.
- Set the system’s limit on the number of failed logins for each login ID.
- Remove a lockout or change the system’s LOCKOUT timer value.
- Set the system’s inactivity timer value.
- Set system security logging and alarm configuration.
- Manage system security logging processes.
- Upgrade security software.
- Terminate any user or system session.

M-27. On each NE/MS, a SYSTEM SECURITY ADMINISTRATOR shall be able to execute all of the CRITICAL SECURITY ADMINISTRATION ACTIONS.

M-28. On each NE/MS, a role other than the SYSTEM SECURITY ADMINISTRATOR shall NOT be able to execute any of the CRITICAL SECURITY ADMINISTRATION ACTIONS unless a SYSTEM SECURITY ADMINISTRATOR has delegated these specific authorizations.

M-29. Each NE/MS shall support the following application security MANAGEMENT ACTIONS:

- Define and assign new user and group privileges at the application level.
- Maintain a record of all requests for login IDs to the application.
- Add and delete users at the application level.
- Monitor all application security logs.
- Configure application security logging and alarms.
- Manage application security logging processes.
- Terminate any user application session.

M-30. On each NE/MS, an APPLICATION SECURITY ADMINISTRATOR shall be able to execute all of the application security MANAGEMENT ACTIONS defined in M-29.

5.3.2 Authentication Defaults

The proper use of default passwords has been discussed at length in security literature. Historically, default passwords ranged from hard coded in the program to a default associated with each software release or upgrade. The following are AUTHENTICATION default requirements.

M-31. One of the following shall apply:

- The configuration software shall create a unique initialization password for each application in the new release or upgrade[18] of the software.
- If a default password is used, the system shall require the replacement of the default password with a unique password before the device goes into service.
- If a device is delivered without a password or a null password, a unique password shall be assigned during the installation process before the device goes into service.

M-32. The system age threshold for login passwords shall be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTRATOR if the functionality is also built into the application. The default shall be 90 days.

M-33. The system inactivity timer value shall be configurable by the SYSTEM SECURITY ADMINISTRATOR or by the APPLICATION SECURITY ADMINISTRATOR if the functionality is also built into the application. The default shall be 60 minutes.

M-34. The system limit on consecutive failed logins for a given user ID shall be configurable by the SYSTEM SECURITY ADMINISTRATOR or the APPLICATION SECURITY ADMINISTATOR if the functionality is also built into the application. The default shall be five.

[18] This is similar to the practice in which each commercially purchased compact disk carries a unique enabling password.

5.3.3 Security Audit Logging

It is important that each NE/MS provide adequate capabilities to allow investigation, audit, and real-time detection and analysis activities, so that proper remedial actions can be taken. This clause considers security audit logs; however, the specific details of the content and format of the security audit logs are beyond the scope of this document.

Note that investigation and forensic analysis activities may include investigation of non-security related OAM&P messages as well as the information stored in the security audit logs described in this section. Logging of non-security related OAM&P messages, sometimes referred to as “recent change” messages, is beyond the scope of this document.

M-35. Each NE/MS shall be able to log any action that changes the security attributes and services, access controls, or other configuration parameters of the devices; each login attempt and its result; and each logout or SESSION termination (whether remote or console).

O-2. Each NE/MS should provide the capability to configure those CRITICAL SECURITY ADMINISTRATION ACTIONS that are to be included in the security log.

It is recommended that audit log entries be sent to an unalterable audit server after being sequence labeled and cryptographically authenticated (signed) by the NE/MS.

M-36. Each NE/MS shall be capable of remote logging over a TRUSTED PATH.

M-37. Each log entry shall contain the following information:

- A description of the action or the actual action that is being logged
- The identity and security level of the user or process that initiated the action
- The date and time the action occurred
- Network source and destination information, if applicable (e.g., when logging in)
- An indication of the success or failure of the activity.

Additional information on logging may be found in ANSI T1.243-1995 (R1999), *Operations, Administration, Maintenance, and Provisioning—Baseline Security Requirements for the Telecommunications Management Network*.

5.4 NE/MS Use and Operation

The requirements in this clause apply to both remote and console access to a NE/MS. These mandatory requirements represent a baseline for NE/MS that actually store user IDs and passwords. Many NE/MS reference a centralized ACS to store user IDs and passwords. The mandatory requirements expressed throughout this document apply to a NE/MS if it holds user IDs and passwords and the user IDs and passwords stored on the ACS.

M-38. Each of the NE/MS shall synchronize time in an authenticated manner (e.g., NTP Version 3).

M-39. For each NE/MS, each MANAGEMENT ACTION shall be associated with a single authorized SESSION.

M-40. Each SESSION shall be established via proper AUTHENTICATION as detailed in requirement M-12.

M-41. Communications between a NE/MS and an ACS for the purposes of conveying AUTHENTICATION credentials shall occur over a TRUSTED PATH.

M-42. Each NE/MS shall use ACCESS CONTROL and partitions to allow, deny, or otherwise control a user, user group, or remote system's access to the NE/MS and shall provide functionality restricting users to the data, transactions, and equipment necessary to fulfill their roles. Access permissions should include, and not be limited to, read only and read-write.

5.4.1 Login Process

M-43. The APPLICATION SECURITY ADMINISTRATOR or SYSTEM SECURITY ADMINISTRATOR shall assign to every individual a unique user ID to log in to an application or host computer system.

M-44. Each NE/MS shall automatically force the user to change their password on the first access after the account has been established and on the first access after the password has been reset.

NOTE: The following requirement (M-44) demands that a distinction be made as it pertains to the management of a Network Element (NE) vs. a Management System (MS). Management of Network Elements requires the monitoring of a device through several mechanisms, perhaps simultaneously, while making configuration changes. In the case of an MS, this is not necessary.

The intent of this requirement is to deny users the capability of consuming all available resources of an NE/MS. Operations staffs should adjust the NE default as needed for individual situations, and should monitor and investigate attempts to exceed these limits, as they may indicate an operational deficiency or an attempt at mischievous activities.

M-45. Each NE/MS shall prevent, control, or limit the simultaneous active usage of the same user ID. The number of simultaneous active sessions shall be configurable on a user ID basis. The Network Element (NE) shall have a default of 6. The Management System (MS) shall have a default of 1.

M-46. The NE/MS application shall work properly without SUPERUSER access privileges for any application roles (i.e., APPLICATION USER/OPERATOR, APPLICATION ADMINISTRATOR, and APPLICATION SECURITY ADMINISTRATOR).

M-47. Each NE/MS shall display to the user during the logon process the time and date of that user's last successful AUTHENTICATION.

M-48. A customizable proprietary information statement and no trespassing warning shall be displayed on the initial entry screen before any logical access is allowed. Equipment should support a minimum length of 1,600 characters. A default message should be provided. The following is an example of a warning banner:

WARNING! This computer system and network is PRIVATE and PROPRIETARY and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network. The owner, or its agents, may retrieve any information stored within the computer system or network. By accessing and using this computer system or network, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the computer system or network, including information stored locally or remotely on a hard drive or other media in use with this computer system or network.

It is recommended that each entity develop an appropriate warning banner.

M-49. Any failed login attempt shall immediately report to the user only that the login process has failed or is invalid. Information such as “invalid user ID” or “invalid password” shall not be reported.

M-50. Each NE/MS shall LOCKOUT a user account from logging in after a configurable threshold number of login failures has been reached. The LOCKOUT shall include the console interface. The LOCKOUT shall NOT include the SUPERUSER account. The default value is five login failures.

M-51. Each NE/MS shall NOT have a mechanism for bypassing the login AUTHENTICATION and logging in processes.

M-52. No NE/MS shall ever display a plaintext password in any media, including displays on terminal screens, printouts, and log records.

M-53. Each NE/MS shall enforce password aging with a configurable threshold.

A common and acceptable implementation of M-51 is for the system to immediately require the user to set a new password after authenticating the user with the old password. Alternatively, the system may require a SECURITY ADMINISTRATOR to properly change the password. If an account has not been used for a period of time, it will be considered dormant.

M-54. If a login password has surpassed the age limit for that system, then the NE/MS shall LOCKOUT the login for that user ID until the password is properly changed. The default age limit is 90 days.

M-55. If an account, including the SYSTEM ADMINISTRATOR account, has been dormant for a configurable threshold period of time, each NE/MS shall generate an alert. The default value is to provide an alert after 120 days.

M-56. If an account has been dormant for a configurable threshold period of time, each NE/MS shall generate an alert and the account shall be DISABLED. The DISABLE process shall NOT include the SYSTEM ADMINISTRATOR account, the SYSTEM SECURITY ADMINISTRATOR account, and the SUPERUSER account. The default value is to alert and DISABLE the account after 180 days.

M-57. A DISABLED login ID shall be re-enabled by at least one of the following:

- A properly logged-in APPLICATION SECURITY ADMINISTRATOR
- A properly logged-in SYSTEM ADMINISTRATOR
- A properly logged-in SYSTEM SECURITY ADMINISTRATOR

The options to re-enable login IDs can be configured as a system-wide parameter at the role level. The default for the parameter allows all options.

M-58. A LOCKED OUT login ID shall be reset to remove the LOCKOUT condition by at least one of the following:

- A properly logged-in APPLICATION SECURITY ADMINISTRATOR
- A properly logged-in SYSTEM ADMINISTRATOR
- A properly logged-in SYSTEM SECURITY ADMINISTRATOR
- Automatically, following the crossing of a configurable timeframe. The default delay must be at least 60 minutes.

The options to remove a LOCKOUT from login IDs can be configured as a system-wide parameter at the role level. The default for the parameter allows all options.

5.4.2 Logout Process

M-59. Each properly logged-in SESSION shall be logged out by the user or by system inactivity.

M-60. Each NE/MS shall log out a properly logged-in SESSION when the time since the last activity for that SESSION exceeds the system's configurable inactivity timer value. The default inactivity timer value is 60 minutes.

5.4.3 Applications

M-61. A user's role type shall remain unchanged during the execution of and exit from any NE/MS application.

The user shall not be able to use a control sequence mechanism, for example, shell escape to a SUPERUSER mode. Or, if the application fails, it must not leave the user in a different role with more privileges. The user must reauthenticate (relog-in) in order to assume a different role.

5.5 Communications

Secure communications are the foundation for securing the MANAGEMENT PLANE in a modern network. Annex A discusses architectures and protocols for implementing secure MANAGEMENT COMMUNICATIONS. The mandatory requirements defined in this clause apply to all interfaces of a TMN as described in the ITU-T Recommendation M.3010, *Principles for a Telecommunications Management Network*.

M-62. For each physical or logical interface that carries any MANAGEMENT TRAFFIC in an NE/MS, the NE/MS shall be configurable to secure MANAGEMENT TRAFFIC with STRONG AUTHENTICATION and cryptographic protection in order to provide confidentiality, integrity, and replay protection.

M-63. Any password transmitted in cleartext shall only be transmitted across a TRUSTED PATH unless a one-time password mechanism is used. If one-time passwords are used, then they may be sent in the clear.

5.6 NE/MS Development and Delivery

Security of an NE/MS is dependent on the complete life cycle process. Security is an issue during conceptual design and remains an issue through detailed design, development, deployment, and decommissioning of a product. Appropriate controls and testing during the complete life cycle process are critical to providing acceptable levels of security. Annex B, clauses B.5.2 and B.5.3, discuss additional life cycle considerations.

M-64. All software delivered to a service provider or other customer shall include cryptographic AUTHENTICATION and integrity protection mechanisms such as digital signatures or symmetric message AUTHENTICATION as specified in clause 5.1.

O-3. All NE/MS receiving software should be capable of interpreting the cryptographic AUTHENTICATION and integrity protection mechanisms and verifying the source and integrity of the software.

M-65. All software updates, including patches, shall be transmitted to the receiving NE/MS over a TRUSTED PATH.

M-66. All NE/MS shall be able to electronically determine their current software and hardware revision levels and validate appropriate software/firmware configurations.

Annex A

(Informative)

A Architectural Considerations and Examples

This annex describes considerations for providing security at each protocol layer. Table A.1 describes the basic alternatives for secure network architectures based on the open systems interconnect (OSI) layers.

Table A.1 – Pros and Cons Based on OSI Layers

Layer	Protocols	Viability	Pros	Cons
1	Physical	None	N/A	N/A
2	Ethernet media access control and logical link control, point-to-point protocol (PPP), and others	Low	N/A	In some cases, encryption is difficult to tie to authentication, authorization, and accounting (AAA).
3	Internet Protocol security (IPsec)	High	Available, minimal device impact possible. Works with any application.	Bootstrapping, installation, and full resets can possibly open vulnerabilities.
4	Secure Socket Layer (SSL)/ Transport Layer Security (TLS)	High	Available, well integrated with public key infrastructure. Allows specific port for each type of traffic (Hypertext Transfer Protocol [HTTP]/SSL: 443, Lightweight Directory Access Protocol/SSL: 636)	Nontrivial interface for each element. Provides only security mechanisms for traffic running over the transmission control protocol (TCP). No protection for user datagram protocol (UDP), real-time transport protocol, or stream control transmission protocol traffic.
7	Simple Network Management Protocol Version 3	Medium	Specific security solution targeted to particular application. Independent of underlying transport.	Difficult to create a seamless architecture. Difficult to deploy in embedded systems.

Security can be added at different layers within the OSI seven-layer model. Usually, security exists at the Application Layer (Layer 7), Transport Layer (Layer 4), Network Layer (Layer 3), or Data Link Layer (Layer 2). These layers are described below.

A.1 Application Layer Security

Application layer security provides a security solution targeted specifically to a particular application, which must be implemented in the end hosts. An example of application level security is a secure shell terminal session that may be used as a secure replacement for Telnet.

Application layer security has the advantage of easy access to user credentials because it operates in the context of the user, which makes user AAA services easier to implement. Also, an application can be extended for security without having to depend on the operating system to provide these services.

The downside of application level security is that security mechanisms must be designed independently for every application that needs to be secured. Thus, it is very difficult to create seamless and scalable security architectures.

A.2 Transport Layer Security

TLS provides security services at the TCP layer. SSL, which is being revised and standardized by the Internet Engineering Task Force (IETF) as TLS, is the security protocol that provides security at the transport layer.

As shown in figure A.1, a single SSL/TLS instance can be used to create multiple SSL/TLS sessions through an Internet protocol (IP) network to provide security for various applications. Modifications are required to each application to allow that application to request SSL/TLS security services. SSL/TLS is the de-facto standard for Web-based HTTP traffic. All standard Web browsers include built-in SSL/TLS technology.

Because SSL/TLS technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services. SSL/TLS is applicable only to TCP traffic and cannot be used to protect UDP traffic.

A.3 Network Layer Security

Network layer security provides security services at the IP layer. The IETF IPsec Suite is the security protocol that provides security at the network layer. IPsec is optional for IPv4 and a mandatory component of IPv6.

As shown in figure A.1, a single IPsec tunnel can be used to protect data from many different applications or transport protocols, or both. No modifications are required to the applications, and the security services appear transparent to the applications. IPsec is the de-facto standard used for creating network layer virtual private networks.

Because IPsec technology does not operate in the context of the user, obtaining user context is difficult, making it harder to implement user AAA services. A human should authenticate himself or herself to the workstation, and the workstation can then act as an authentication proxy for the human to other systems. Authenticated operator IDs can be logged as part of the command execution for nonrepudiation. Use of multiple-user IPsec tunnels weakens attribution to a single individual and acts as a “backdoor” into networks, weakening defense-in-depth measures such as firewalls and intrusion detection systems.

A.4 Data Link Layer Security

If two devices are connected by a data link (e.g., Frame Relay, PPP, or Ethernet) and all the traffic between the two devices needs to be encrypted, then data link encryption can be used to provide confidentiality. The data link encryption can be provided by the end devices or by external encryption devices. Encrypting traffic can slow the rate of the data traffic flow but using hardware link encryption provides less of a bottleneck than applying network layer confidentiality services; however, this solution is not scalable. This solution only works well for devices connected by a common Layer-2 technology (e.g., Ethernet, PPP, or Frame Relay). A disadvantage of this solution is that each link in the network has to be encrypted separately and the information is not protected once it leaves a particular link.

Layer 3 Security (IPSec)

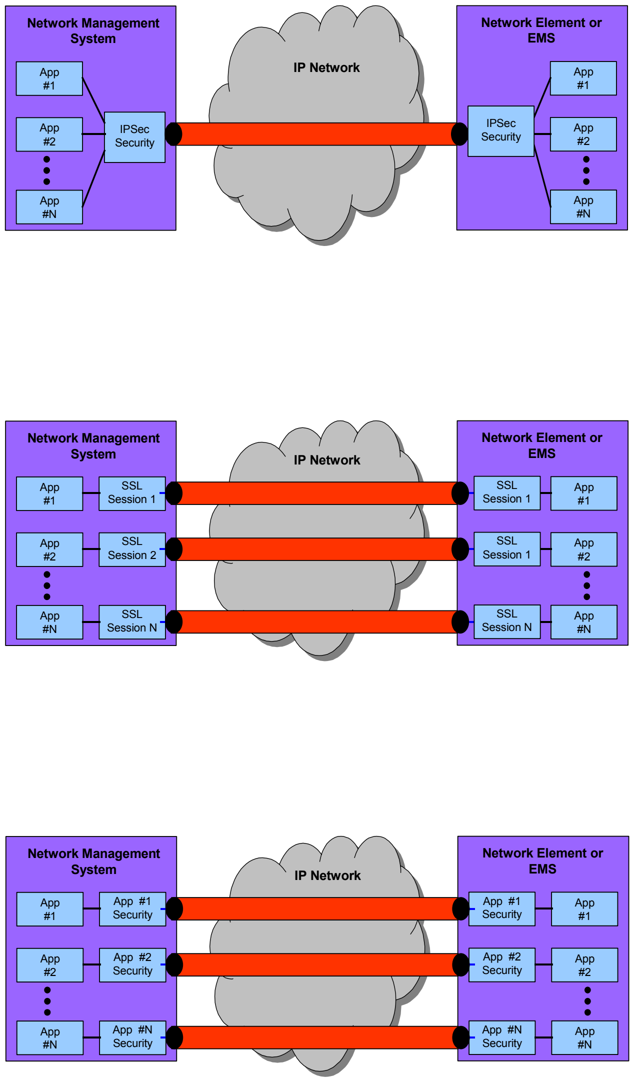

Figure A.1 – Security at Different Layers in the OSI Model

Annex B

(Informative)

B Additional Security Considerations

The security procedures detailed in the subsequent clauses are tutorial in nature. They are outside the scope of detailed requirements provided by this document, but should be considered to provide a secure system. In some cases, mandatory language is used; however, this is provided for informational purposes and should serve only as an example. Protocols and recommendations included in this annex are subject to future discussions and contributions. They do not represent any intent to include or exclude content in existing or emerging standards.

B.1 Applicability to Enterprise Operations, Administration, Maintenance, and Provisioning

Enterprises today have evolved beyond the traditional isolated enterprise networks of the past. Enterprises have grown to multi-site businesses that span large geographical areas requiring extranet network connection to customers and business partners. Enterprises must allow partners and customers to gain access to internal data and make operational business decisions based on this data.

Enterprise networks are developed and administered by the enterprise itself or have been purchased as a managed network from a network provider. Services being developed by providers will allow the enterprise to manage their portion of a larger network environment. These services are based on national and international standards.

As the industry moves forward, requirements for access to fault and performance data, and the ability to configure various components of the network by the contracting enterprise, necessitates that appropriate security mechanisms are in place. These mechanisms must provide adequate control for protecting not only the enterprises' managed network, but also providers' own internal network. The internal network may be interconnected to these enterprise networks and may be a part of the national telecommunications infrastructure. In summary, the security requirements for operations, administration, maintenance, and provisioning traffic outlined in this document are fully applicable to enterprises and service provider/carrier networks.

B.2 Common Object Request Broker Architecture, Simple Network Management Protocol, Extensible Markup Language, and Simple Object Access Protocol

The following considerations should be taken into account with regard to security for common object request broker architecture (CORBA), simple network management protocol (SNMP), extensible markup language (XML), and simple object access protocol (SOAP). In addition, there are other protocols that may be equally applicable such as the blocks extensible exchange protocol. Although no changes to these evolving protocols are proposed, the following discussion could be used to enhance security.

B.2.1 CORBA

The CORBA Security Service comprises the security functionality of authentication of principals (human users and objects), authorization of access to objects by principals, security auditing, communication security, nonrepudiation, and administration. All of this may be overkill for many applications, though. Instead, applications might require only the communication security and system-level authentication functionality based on transport layer security (TLS) technology (and its precursor, secure socket layer [SSL]) for availability and simplicity reasons. Finally, some applications might require no security. The optional requirements below, therefore, reflect three possible choices:

- No security

- Object request brokers (ORB) use TLS (or SSL) to provide communications security and system-level authentication, which is essentially "session" security

- ORBs use the CORBA Security Service to provide communications security, authentication, nonrepudiation, and access control lists for groups or individuals accessing individual objects and operations

Additional information on security in the CORBA framework may be found in International Telecommunication Union – Telecommunications Sector (ITU-T) Recommendation Q.816, *CORBA-Based Telecommunications Management Network (TMN) Services* and ITU-T Recommendation Q.816.1, *CORBA-Based TMN Services Extensions to Support Course-Grained Interfaces*.

If CORBA is used in the network element/management system (NE/MS) interfaces, then CORBA security mechanisms should be applied. Conformance level of the CORBA security implementation should be clear. The following discussion provides guidance regarding CORBA security. No attempt to identify standards should be inferred. When supplying products or systems based on CORBA, the basic security levels are as follows:

- Level 0: No application security is provided, and programs are security unaware. Authentication, encryption, data integrity, object invocation authorization, audit trails, and security domain administration should be provided.

- Level 1: Programs may be security aware, which means that they may call an application programming interface for access to additional services such as verification of signatures, check access to objects, and write audit records.

- Level 2: Provides support for digital signatures permitting signing and nonrepudiation of transactions. This is particularly important when operating across various organizations— for example, in a business-to-business context or network management peering arrangement.

The Common Secure Interoperability (CSI) Specification defines standards by codifying the specification for secure interoperability when using General Inter-ORB Protocol/Internet Inter-ORB Protocol:

- CSI Level 1: The identity of the initiating principal is communicated from sender to receiver.

- CSI Level 2: The identity of the initiating principal is communicated from sender to receiver, but the identity can be delegated to other objects so that other objects can impersonate the user.

- CSI Level 3: In addition to identity being passed, the attributes of the initiating principal passed from client to target may include other authorization information, such as membership of roles or groups.

It is incumbent on suppliers to—

- Be fully conversant with the security capabilities of the ORB technology selected,

- Ensure it meets the requirements for security outlined elsewhere in this document.

As its name implies, CORBA deals with objects. Object security is about preventing the unauthorized use of objects by enforcing a set of access control rules. CORBA security ensures users are accountable for their actions on or with an object and ensures the availability of objects.

Object security differs from many other aspects of security. Frequently, the developer does not need to know security details because security is applied at a later stage as with a wrapper. Therefore, certain aspects are vitally important. In CORBA, names may be duplicated or may not exist at all; only reference numbers may exist. It should be possible to define an object's policy without knowing the object's name. Similarly, it must be possible to define an object's policy even on objects with many names, and the policy must be applied regardless of the name used to secure the object.

Typical object-oriented systems have tens of thousands of objects, and it is not reasonable to expect security to be defined for individual objects. Therefore, it should be possible to group together objects and define a policy for the group of objects whose protection needs are similar.

- *End-to-End Authentication:* CORBA can pass the user context to another application. Where a strong trust relationship has been established between these systems, it may be possible to accept this information without further verification. However, where other mechanisms do not exist, it may be necessary for the security of other systems to be tightly coupled with CORBA security. End-to-end authentication is very important, and it is worth checking whether the vendor supports this.

- *Access Control:* CORBA supports the idea of role-based login. Systems should always be developed using this feature because not only does it reduce costs of administration; it simplifies it, which means that the configuration is less likely to have errors.

- *Encryption:* Use of encryption within CORBA must comply with the requirements stated in this document. Full use should be made of CORBA features for integrity, confidentiality, and origin authentication, especially when communicating over a network of any type.

- *Policy Administration:* CORBA policy administration is responsible for setting up information about domains, users, roles object access policy, message protection policy, and audit policy. Clarity should exist throughout the design of all aspects of domain and object naming. Roles should be clearly defined with the aim of ensuring appropriate segregation of duties.

B.2.2 SNMP Security

SNMP, a widely used method of administering a variety of processor-based equipment, offers the ability to—

- Obtain device configuration parameters

- Set device configuration parameters

- Send alerts from the managed device to a central analysis system.

Many deployed versions of SNMP have significant security vulnerabilities. In Versions 1 and 2, the password (known as the community string) is transmitted in clear text. In addition, although checks may be made to validate the Internet protocol (IP) address of the client, a moderately determined attacker can spoof IP addresses. Versions 1 and 2 of SNMP create significant security exposures in several networks. Therefore, SNMP Versions 1 and 2 should be used only as a last resort. ITU-T Study Group 4 is considering the establishment of two new protocol stacks:

- SNMPv3 or V2C with TLS over transmission control protocol (no access control), and

- SNMPv3 with user security model over user datagram protocol (as a forward looking stack).

Where SNMP is deployed, Version 3 is the preferred level. SNMP Version 3 is more secure and should be used in all new systems because it provides protection against modification of data, masquerade, re-ordering of messages, and loss of confidentiality. The following countermeasures should be considered to secure SNMPv3 access to NEs:

- An SNMP agent should send an alert to a manager if it receives a command originating from an unknown source.

- Access controls should be used to allow SNMP messages only from an authorized manager. SNMP messages from all other sources should be denied and treated according to appropriate security policies. It may be desirable to block unauthorized requests at the device and at a network perimeter.

- The default community string should not be used.

- Access violations and access errors should be logged.

- SNMPv3 uses the data encryption standard as default; however, more secure algorithms can be used.

- SNMPv3 should be used at least with AuthNoPriv, which provides authentication but no confidentiality of transactions. Preferably, AuthPriv will be used.

- SNMP agent logging should be enabled.

- Any service or capability not explicitly required should be disabled, including SNMP if it is enabled.

- SNMP traffic should be segregated onto a separate management network.

B.2.3 XML

The XML standard provides language for defining data structures. The current standard is 1.0. Version 1.1 is a candidate recommendation under review. The Organization for the Advancement of Structured Information Standards' (OASIS) Security Services Technical Committee is seeking to broaden security functionality by leveraging XML. OASIS is working on finalizing security assertion markup language (SAML). SAML is based on four assertions:

- *Authentication*—issuer has authenticated the object,

- *Attribute*—specific uniform resource identifier or extension schema that defines the attribute,

- *Decision*—reports validity of authentication, and

- *Authorization*—subject has permission to access resource(s).

The XML assertions must include the following:

- *Basic information*—unique identifier or name for the assertion and commonly includes date and time of issue and validity time span,

- *Claim*—a document describing the use of the assertion,

- *Condition*—the assertion may be subject to conditions that make it valid or invalid, and

- *Advice*—provides additional information such as assertions used to make a policy decision.

B.2.4 SOAP

SOAP 1.1 is the current recommendation form the World Wide Web Consortium. SOAP is a message format not tied to a specific protocol. It most commonly uses hypertext transfer protocol (HTTP), but can use other protocols such as SMTP or file transfer protocol (FTP). When SOAP is used with HTTP, the firewall views SOAP as HTTP and usually will allow it to pass. SOAP could potentially be filtered by the firewall, even when the firewall is not aware of SOAP. This filtering, however, is not an easy task and is susceptible to errors. Filtering is a challenge because encryption can hide the content and context of the data transported (i.e., XML), and SOAP has no uniform addressing scheme or internal structure (i.e., headers and method names are optional).

B.3 Communications Assistance for Law Enforcement Act

Telecommunications carriers should take the following security considerations into account with respect to the implementation of the Communications Assistance for Law Enforcement Act (CALEA). The basic CALEA requirements for systems security and integrity can be found in Title 47 Section 1004 of the US Code [47 USC Sec. 1004]. Further requirements on telecommunications carriers for support of lawfully authorized electronic surveillance (LAES) under CALEA can be found in the relevant rulemaking proceedings of the Federal Communications Commission (FCC) and the Department of Justice (See http://www.askcalea.net/regulatory/). Related industry safe harbor standards such as TIA/EIA/J-STD-025-A-2000, *Lawfully Authorized Electronic Surveillance*, December 1, 2000, define the interface between the carrier and the law enforcement agency but do not provide specific security requirements on the carrier's operation or equipment.

Security requirements and practices required under CALEA are explicitly set forth in "Subpart V-Telecommunications Carrier Systems Security and Integrity Pursuant to the Communications Assistance for Law Enforcement Act," Title 47 of the Code of Federal Regulations [47 CFR §§ 64.2100 et seq.]. Section 2105 [47 CFR § 64.2105] requires submission by carriers of their systems security and integrity policies and procedures to the FCC. Section 2106 [47 CFR §§64.2106] addresses penalties for failure to comply with the requirements set forth in Sections 2103 and 2104. However, Title 47 does not specify the technical means for securing the surveillance.

Telecommunications carriers may wish to reference Telcordia Technologies generic requirements specifications GR-2975-CORE, *Surveillance Administration System Generic Requirements*, September 2000, and GR-2973-CORE, *Lawful Access Feature: Switching Generic Requirements*, April 2000. These specifications provide practices for identification, authentication, system and resource access control, alarm management, security log (audit), and security administration.

Security practices for LAES activities should be robust and the same as for any critical NE, operations support system (OSS), or MS with some exceptions as listed below. As required in the FCC regulations, these practices relate to the necessity of keeping LAES activities confidential.

- Only authorized employees will participate in LAES activities.
- LAES information, including target identity, law enforcement agency(ies) involved, call content and call-identifying information will be protected from disclosure to unauthorized personnel.
- Only authorized personnel will have access to LAES commands and processes.
- An up-to-date list of personnel authorized to access, maintain, administer and manage LAES activities, processes, and procedures will be maintained.
- LAES security activities, policies, and procedures will be adequately documented and made available to authorized personnel.
- LAES-related security logs and activity records will be maintained and stored in a secure facility.
- A rigorous documented process will be implemented to identify and authenticate law enforcement agencies and process lawful intercept requests.

B.4 Physical Security Considerations

The following considerations should be taken into account for physical security. When preparing security requirements, physical security is an important component. Most security architecture's assume that the physical environment is protected. At one time, all NE were contained in central office (CO) buildings. These buildings had employees working around the clock to operate, provision, administer, and maintain this equipment. Employees knew each other, and outsiders could not gain access to the sites without someone noticing and challenging them. However, the environment is very different today. Many, if not most, COs are unmanned and dark most of the time. Roving crews and individuals who are dispatched by a central location perform scheduled upgrades and maintenance tasks. Today, 24 X 7 security guards are the rare exception. COs are also used by outside plant personnel as a convenient place to meet and store tools and equipment. The following are characteristics of a secure facility:

- All personnel entry and exit is logged and recorded.
- Vendors and co-located personnel are vetted and their entry/exit is logged and recorded.
- Physical access to NE is limited to authorized employees.
- Co-located personnel are subject to the same access requirements as the incumbent service provider.
- No one who has legitimate physical access to the building has logical access to NEs, consoles, network access device's OSSs without protected authentication.
- Unauthorized access will be detected and responded to in a timely manner.
- Services such as water, power, and telecommunications will be available.
- Sites are under surveillance by random roaming security personnel, alarm systems that monitor and record door and window openings and closings, motion detectors, and inferred detectors, and remote video monitoring of critical locations.
- Retention of surveillance media and logs should be documented. Length of retention would vary depending on risk level.

The following clauses provide additional information regarding physical security. A detailed description of physical security issues can be found in the National Communication System, *Public Switched Network Security Assessment Guidelines*, September 2000.

B.4.1 Physical Premises Security

Organizations will usually implement various levels of building access controls in accordance with the importance of the assets resident in the facility. Often, large corporations will build separate high-security facilities for critical network components, such as switches or data centers. The importance of the assets resident there determines the level of security. This determination comes during a discovery phase and asset assessment review. The following clauses include assessment items for a facility housing high-value or critical assets. Less strenuous reviews would be undertaken for less sensitive facilities. The overall physical security assessment must determine the level of protection needed and the relative quality of the protective mechanisms in place.

B.4.1.1 General Building Security

Although a building's doors and windows are usually considered to be its primary access points, other points (e.g., air vents, entry points for water, gas, communications, and electricity, and drainage conduits) must be considered, depending on the kinds of threats. Additional entry points such as CO cable vaults need to be considered, as do other places where the potential to cause damage exists. Furthermore, the buffer space between the public and the building itself must be considered. Lawns, landscaping, lighting, and fences can contribute to the first layer of perimeter defense because they slow or prevent covert approaches. Physical barriers such as concrete posts or large concrete landscaping planters can be used to prevent approach by cars, trucks, or other vehicles with the potential destructive intent. Outside cameras and other surveillance gear further enhance or enlarge this buffer space.

B.4.1.2 Guards, Locks, and Identification Badges

Building guards protect the external perimeter of the building and sometimes protect internal areas. For critical facilities, the review should ensure the following:

- All doors providing access to the facility are either locked or guarded at all times.

- Any doors not normally in use, such as emergency exits, are alarmed. The review should ensure that alarms function properly and procedures exist to respond to alarms.

- Doors are installed properly so that they cannot be removed from the outside (e.g., hinges and bolts are protected from outside tampering).

- During peak periods of ingress and egress, entrances and exits have a guard present. During off-peak times, the door should be monitored, and some other form of access control should exist (e.g., swipe cards, proximity cards, and keys).

- Access through unguarded doors uses a method requiring identification of the entrant.

- Unguarded doors that provide access via keys or other means have mechanisms to prevent "tailgating."[19] Mantraps, revolving doors, and detectors can be used to prevent tailgating or send an alarm that tailgating has occurred.

- The recruitment qualifications, training, and retention methods used for employing guards are adequate and appropriate. This is particularly important for contracted guard services, which are common.

- Employees, onsite vendors, contractors, and other authorized individuals possess and display a badge at all times while in the building.

- Non-employee visitors are given a temporary identifier, such as a visitor's pass, and are required to display it clearly.

- Procedures and conditions exist under which visitors can enter and work unescorted, and the conditions under which they must be escorted.

- Employee badges display a color photograph. The photograph should be big enough that the employee need not have to hand the badge to a guard for the guard to see it. It should be constructed so that the photograph cannot be altered or replaced. The photograph should be clear enough that the guard could compare the picture with the face of its wearer.

- The badge displays the employee's name and any other identifying information (e.g., number, bar code) clearly.

[19] Tailgating refers to an unauthorized person's act of following through a door opened by an authorized person.

- The badge has a mark or indication that distinguishes employees from non-employees with access to buildings.

- The badge is durable and resistant to wear, damage, or alteration as much as possible.

- The badge contains electronic or magnetic information that may be needed by card readers.

- The badge may include a smart chip that embeds additional information, such as biometric data or X.509 certificates.

- Badge authentication and authorization systems should be linked to a central security directory to allow immediate change or removal of access privileges.

- The badge supports a capability to limit access to some areas of the corporate campus, as opposed to full access, when appropriate.

- The badge has an address to which it can be mailed without postage, if lost, if a non-employee were to find it.

- Corporate or building security can disable or invalidate any badge that has been lost or whose wearer is no longer permitted to enter the building or corporate campus.

- When the wearer terminates employment, someone (manager, building guard, corporate security) will retain or destroy the badge so that it cannot be used illicitly.

Guards are not the only personnel responsible for preserving the internal security of a building. Authorized occupants often enhance building security by vigilance and passive monitoring. The assessment should determine whether the staff has been empowered to challenge unauthorized personnel in controlled areas. A penetration test can be valuable for ascertaining the degree to which guards and employees are appropriately trained in the importance of physical security. Reviewers may attempt to sneak past or talk their way past guards or to entice employees to provide admittance through unguarded entrances.

B.4.1.3 Physical and Logical Key Administration

Traditional physical keys are rarely used in sensitive facilities because they are difficult to inventory and recover and they do not provide an audit trail of the user. Often, the use of physical keys is restricted to access to internal portions of the building, such as storerooms, custodial rooms, and wire closets. It is still common, however, to find businesses and installations that use key locks as their primary means for ingress to buildings or access to critical areas within buildings. When that is true, the following actions are important:

- Procedures exist for authorizing distribution of keys to individuals, including key control and logging of access and distribution

- Keys be individually numbered

- A complete inventory of keys and their owners be maintained and audited

- Criteria be in place for replacing locks when keys are lost

- Periodic audits of the key inventory be enforced and procedures for reconciling discrepancies be in place

- Procedures are in place for recovering keys when access is no longer needed or authorizations change.

Logical key (e.g., proximity cards) procedures must be evaluated against the same criteria. Key recovery, ingress and egress recording, and authorization procedures are simplified with logical keys because these systems provide central facilities for monitoring use, assigning authorization, and disabling of keys. Still, procedures must be in place to ensure that those responsible for maintaining the key inventory and authorization database are notified when individuals leave or their access requirements change. Combination locks, a special case of logical locks, should be assessed to ensure that combinations are not discernible from wear patterns or from combinations written down. Combinations should be changed if entry authorizations are changed.

B.4.1.4 Functional Separation of Facilities and Multilevel Access Control

Physical security applies to internal portions of a building as well as the external perimeter. Access to internal areas that are considered sensitive or operationally critical should be controlled when access to their contents is limited for any reason (e.g., they contain sensitive data, experiments, or equipment). In general—

- Critical computer and network facilities should be contained in areas having separate physical access control mechanisms. Access should be granted only to those having a need.

- Procedures should be in place to ensure that proprietary information is kept in secure facilities when not in use. Offices and file rooms where such material is routinely kept should be locked. The cabinets in which proprietary information is kept should also be locked.

- All potential access points to critical computer and network facilities (e.g., consoles, operations centers) should be controlled in a manner commensurate with the control enforced over the facility itself.

- A record of access to all such controlled spaces should be maintained.

- Storage media holding critical information should be encrypted or housed in locked, limited-access areas.

- A critical system's physical address should not be disclosed to those not having a need to know.

Controlling the internal areas of a building can be enhanced through the use of segregated roles and responsibilities. For example, administrative staff does not require access to an organization's computer rooms. Likewise, engineers do not generally require access to the document control room. The review should assess whether existing functional segregation is appropriate. In addition, dual entry key or combination locks can be used if the degree of risk so indicates.

B.4.2 Building Services

An organization's operations are critically dependent on the availability of services, such as water, power, telecommunications, and waste disposal.

B.4.2.1 Utilities (Water, Power, Telecommunications, and Waste Disposal)

Without water, power, telecommunications, and waste disposal services an organization cannot operate effectively, if at all. Dependency on these services is often undervalued. The assessment should evaluate the organization's planned reactions to service interruptions. For services critical to the continuing function of the business, the following steps are essential:

- Power feeds should be duplicated and geographically separated to prevent accidental loss of power.

- Emergency power should be available to allow the continued operation for greater than the average duration of power outages. Generating capacity should be available for deployment before emergency supplies are exhausted. (Mobile generators may be owned or contracted.)

- Sufficient onsite water storage (or delivery services) should be available to support continued operation of critical components of the facility.

- Outside communications must either have active-standby backups, or must be robust enough to operate in a crisis, as must internal communications. Capacity should be sufficient to handle crisis-level traffic.

- Restroom and sewage facilities must function through crises, or temporary arrangements must be in place (at least contractually) for quick activation.

- Air conditioning for computer rooms and other areas that require controlled environments must be backed up to prevent machine failure or damage from overheating.

- Locked containers for disposal and destruction of proprietary information should be readily available wherever such material is used. The review should trace the disposal path of such material to ensure that it is closed.

Of interest for the assessment is the distribution of these services within buildings. The assessment should evaluate the overall resistance of the facility to service interruption from the origination of the service at the utility provider to the distribution paths inside the building.

B.4.2.2 Emergency Facilities

The review should assess the adequacy of emergency facilities such as fire detection and suppression, power conditioning, air conditioning, ventilation, and other environmental protection systems necessary for continued operation of critical systems. These systems must react in ways that allow—

- People to evacuate the premises

- Equipment to be protected (at least long enough for fire companies or others to arrive)

- Facilities to retain structural integrity

- The building's contents to be protected from the outside environment, as much as possible.

Emergency facilities are important as much for the aftermath of a security breach as they are for accidents and natural disasters, as suggested in the previous clause.

B.4.2.3 Transport Redundancy and Physical Protection of Critical Facilities

Critical computer and communications systems facilities should be geographically dispersed to the extent possible without unduly affecting operational costs, performance, and security. In addition, routing of critical communications links (e.g., important interoffice trunks, signaling links) should be redundant and geographically dispersed inside and outside the facility so that communications may be immediately rerouted over physically diverse backup routes when necessary. The communications networks required for maintaining service should be designed in such a way that no single point of failure will result in a widespread or serious outage.

B.4.3 Environmental and Geographical Threats

Critical sites should be reviewed to identify any risks resulting from their location in areas likely to experience natural disasters, serious accidents (e.g., chemical spills, gas line explosions), power interruptions, and related problems. The review should also consider the effects of simple environmental factors, such as extreme heat or cold, damage from salts and pollution, and harsh climate conditions.

Geographical issues include the reactions of the local populous, such as acts of hostility, responsiveness of local emergency services, and the level of safety afforded to staff, on site and en route to the facility. Because human activities and motivations change over time as a result of unrest, political problems, religious views, or other factors, reviews should be repeated periodically according to a predetermined schedule. Although it is often impractical to abandon facilities where such risks exist, it may be appropriate to duplicate or relocate critical systems and resources housed in high-risk facilities.

Business continuity and disaster recovery plans should be developed that address responding to events resulting from these threats and issues. Plans should include command, control, and communications procedures and should be tested on a regular basis. Operations recovery plans should also include provisions and contracts that can be quickly executed in response to hazardous material (HAZMAT) incidents. These plans should also consider that complete restoration to a safe environment might prevent normal access to the facility over an extended period of time. Potential remediation may require relocating to a backup facility or the availability of HAZMAT trained and equipped personnel to operate the facility during the interim.

B.4.4 Co-location Procedures

The Telecommunications Act of 1996 (also known as the Telecommunications Reform Act [TRA]) mandated that Incumbent Local Exchange Carriers (ILEC) offer various components of their networks to competitors in an unbundled and nondiscriminatory manner. Co-location, a logical result of the mandate, refers to a situation that prevails when plant belonging to multiple providers is present in the same physical location. Of particular concern for the purposes of physical security reviews is that providing such access often means that competitors (sometimes multiple competitors) will require access to physical components and facilities of the ILEC.

For example, physical co-location is the predominant way that ILECs provide facilities for unbundled loops under the TRA. Co-location for the purpose of providing unbundled loops can expose other functional components to misuse or abuse to the extent that their facilities are housed on the same premises. Consequently, extra care must be taken when performing a physical security review of facilities with co-located providers. The review should note that—

- Physical barriers should isolate critical equipment; however, co-located personnel are subject to the same access requirements as the incumbent service provider.

- Key distribution, accounting, and auditing procedures are in place. Processes should be in place to ensure that personnel changes can be monitored across co-located companies.

- Critical equipment and facilities do not draw attention to themselves. The traditional method of clearly marking crucial equipment and transport facilities (so-called "red blocking"[20]) becomes a potential hazard in an open environment and should be avoided.

[20] Red blocking alerts support personnel that the circuit is especially important and that care must be taken not to disturb it accidentally.

B.5 Development Process

B.5.1 Bootstrapping, Installation, and Failure Modes

The following considerations should be taken into account for bootstrapping, installation, and failure mode security procedures.

Several distinct efforts must be completed to secure an implementation from a “new installation” through the implementation’s lifetime. To address these issues it is important to begin by understanding the threats to an implementation. These threats are referenced in ANSI T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning—Security Framework for Telecommunications Management Network Interfaces*, and ISO/IEC DIS 10181 *Open Systems Interconnection—Security Frameworks for Open Systems* standards documents. General connectivity to open systems broadens the threats, which include the following:

- Bootstrap viruses
- Unauthorized access
- Masquerade
- Threats to data integrity
- Threats to confidentiality
- Denial of service (DoS), and
- Repudiation.

B.5.2 Patching Process

Service providers contract with vendors who develop and provide both an application and a platform on which an application is installed, or only application software. In the latter case, providers install the software onto a platform they have previously purchased.

Vendors develop patches to correct or modify operating system (OS) or application software, or both, between general releases. Following appropriate testing, a patch is released to the service provider. In some instances, an application software vendor may release patches in “bundles,” perhaps with some contractual regularity. Releases every six months are not uncommon.

An OS patch generally should not affect the manner in which an application runs; however, that is not always the case. Consequently, when a platform vendor releases an OS patch, it is incumbent on the provider to verify with the application vendor that the OS patch released will not adversely affect the running of the/an application.

In a situation where an application vendor supplies both an application and a hardware platform but is not an original equipment manufacturer (OEM) of the platform, and an OS security patch is released by the OEM of the platform, it is incumbent upon both the application vendor and the service provider to be aware that a security patch has been released and to make arrangements for the patch to be tested in a timely manner, in order to verify that the patch will not adversely affect the application.

The application of security patches must be assigned a priority for review by the application vendor (a matter of weeks versus months). As such, a routine process must be established such that when a provider communicates a concern regarding a security patch to an application vendor, the vendor will take appropriate action in an expedited manner. In addition, the vendor will ensure that installation of the patch will not corrupt previously installed security patches.

If security patch testing reveals an impact to an application, appropriate corrective actions must be taken in a timely manner to identify the issue and formulate plans to correct the condition causing the application to fail, and to subsequently apply the security patch.

The following security considerations should be taken into account when implementing patches to the OS or application software.

- Equipment vendors or system integrators should provide security reference and training manuals for administrators that include details of OS and application security functions and procedures and user access procedures.

- OS security and other patches should be verified as compatible with NE and MS applications.

- OS software: Only patches approved by an OEM should be applied to an operational network element or management platform operating system.

- Management application software: Only patches approved by an original management application vendor should be applied to an operational management application.

- High-impact patches should be distributed in a timely manner and not be constrained by periodic patch dissemination processes.

- All downloads or uploads of any software or configuration data must be secured with strong data origin authentication and strong integrity protection. Ideally, both would be provided through the software provider's digital signature. In addition, the software provider may choose to encrypt the software or configuration data.

- A description of the procedure(s) for acquiring and incorporating the latest security patches for the system and application software executing within each element should be provided at time of delivery.

- A description of the process for testing each security patch, before approving release to the service provider, should be provided at time of delivery.

- The level of backward compatibility of the system software releases and security maintenance patch releases should be specified at the time of delivery.

- System software or a process must track applied patches and upgrades. Patch and upgrade status should be auditable.

B.5.3 Development Life Cycle Security

Security of a product or service is dependent on the complete life cycle process. Security is an issue during conceptual design and remains an issue through detailed design, development, deployment, and decommissioning of a product. For products or services dealing with sensitive information, security may be required even beyond the decommissioning of the product or service. Appropriate controls and testing during the complete life cycle process are critical to providing acceptable levels of security.

B.5.3.1 Personnel Management

A fundamental issue of security that is often overlooked is the trustworthiness of the staff. All staff with access to design, development, and testing must be trustworthy.

- All personnel, contractors, subcontractors, consultants, and employees involved in developing and testing critical software components must pass a background check.

B.5.3.2 Security Awareness and Training

All personnel must be aware of security policies and procedures and the need to protect information assets. The weakest link in security is often the people involved. Security awareness and training dramatically strengthens the weakest link. Awareness reduces the number of unauthorized actions attempted by staff; increases the effectiveness of protection controls; and helps avoid fraud, waste, and abuse of computing resources.

- Security awareness and training should be provided to all staff, including contractors, subcontractors, consultants, and employees.

B.5.3.3 Risk Management

Risk management is fundamental to information security. Risk management is defined as the identification, analysis, control, and minimization of loss associated with an "event." The primary steps identifying risk include identification of actual threats, consequences of a realized threat, potential frequency of occurrence of a threat, and the likelihood of a realized threat. Risk management not only involves performing risk analysis with a cost benefit analysis of protections but also implementing, reviewing, and maintaining protection.

A risk analysis identifies the risks and provides a cost-benefit justification of countermeasures. This information is used to influence the decision making process of all life-cycle phases, including site selection, building design, and construction decisions. To determine if a safeguard is warranted, the annualized loss expectancy (ALE) is determined. The (ALE before safeguard implementation) – (ALE after safeguard implementation) = value of safeguard. Note that the safeguard implementation should include the annual cost for operation and maintenance.

- A risk analysis should be performed for each new product or service. This analysis should include a formal document outlining the approach used and results of the analysis. At a minimum the report should identify all data accessible and the data owner (i.e., corporate, Internet service provider), quantify or qualify the value of the data or service at risk, and determine potential upstream and downstream impacts of the threat to NEs or OSSs.

B.5.3.4 Requirements

- Security requirements should be documented during the requirements gathering phase for the product or service.

B.5.3.5 Design

- Security requirements should be addressed at the design phase, not added after development has begun.

- A security design review should be performed to locate design flaws that affect security.

- All access points into the system must be well documented and provide support for identification and authentication.

- Maintenance backdoors or trap doors that violate the security policy must NOT be allowed.

B.5.3.6 Separation of Duty

Functions that are harmless in a trusted environment can create security vulnerabilities when used in untrusted environments. For example, a postscript interpreter was designed to view documents. An untrusted document could use the functions within the postscript interpreter in malicious ways, such as making copies or deleting files.

- The system should support at a minimum three user levels: user, system administrator/operator, and security administrator.
- Each function should have the minimum level of privilege required to perform the job function.

B.5.3.7 Implementation

- Reused resources should be purged of any information before re-use (i.e., files, memory, and temporary storage).
- Developers should follow best practices for secure programming (i.e., manage buffers so that buffer overflows do not occur).
- Periodic security audits should be performed of the development, test, and support environments.
- Development environments should not be used for non-company business.
- Public domain software should not be imported, used, or distributed for use on development, test, or support systems unless it is available in source code and the source code has been inspected for malicious code.

B.5.3.8 Documentation

- Documentation should be marked with proprietary markings, where appropriate.
- The end-user documentation must describe the security functionality that is not transparent to the user, explain its function, and provide guidelines on use.
- The system administrator's guide should include the following:
  - Cautions regarding functions and privileges that need to be controlled when running in secure mode
  - Document use of audit functions
  - Procedures for examining and maintaining audit logs
  - Detailed audit log structures
  - Procedures for audit log backup and deletion
  - Procedures for checking amount of free space available for audit logs.

B.5.3.9 Operating System

The OS must be able to provide effective hardware and software controls to provide protection appropriate to the value of data and resources being managed. For the proposed security architecture, it is assumed that the OS will provide the security level required for the data and resources being managed. This assumption may need to be reviewed for specific service provider needs. For example, the Department of Defense might have stricter OS security requirements. If the OS does not meet the security provider's security needs, then the software may need to be ported to another OS that supports higher levels of security.

- The OS must have relevant security patches installed.

- The OS must be configured securely and must be delivered with a restrictive security access privilege configuration. There are several documents and Web sites that discuss OS security. Although it is beyond the scope of this document to list them, some examples include the Trusted Computer System Evaluation Criteria,[21] the Common Criteria, and OS Protection Profiles.[22, 23,24, 25]

- Only a minimum of services will be enabled that are required for operation by default.

B.5.3.10 Software Engineering

Security is an integral part of software engineering. To develop a secure product, secure programming techniques and secure protocols must be used. Non-secure programming techniques can circumvent the best security protocols and mechanisms. For example, if a programmer does not manage buffers properly, a buffer overflow may occur and provide more privilege to a user than is appropriate.

- Vendors should follow formal documented development processes, such as the Capability Maturity Model developed by the Software Engineering Institute. Secure programming best practices must be followed in design, development, testing, and distribution of the software.

B.5.3.11 Availability and Performance

Availability and performance are integral to a secure system. Performance can be degraded to the point that the system is no longer usable.

- Design, development, and implementation should minimize the effects of a DoS attack.

- Design, development, and implementation should ensure high availability.

- The network architecture and implementation should have no single point of failure.

B.5.3.12 System Software

The software used to operate and maintain the computer systems (OSs, utilities, and MSs) must be able to be configured and maintained securely. Testing should be conducted to provide assurance that components and security features have been robustly implemented and correctly configured.

- System software and middleware products must be installed and configured securely, including installation of security patches. The software must be delivered with a restrictive security access privilege configuration.

B.5.3.13 Transmission

- The option to secure data transmissions must be available to be used at the service provider's discretion. Secure transmissions options should be available for both client-to-server and system-to-system.

[21] Department of Defense Standard 5200.28, *Department of Defense Trusted Computer Security Evaluation Criteria*, December 1985.

[22] The Common Criteria is becoming the internationally recognized standard to replace the Trusted Computer Security Evaluation Criteria (http://www.commoncriteria.org).

[23] Information Assurance Technical Framework Forum Operating System Protection Profiles, http://www.iatf.net/protection_profiles/operating_systems.cfm

[24] Department of Defense Computer Emergency Response Team, http://www.cert.mil/

[25] National Institute of Standards and Technology, Computer Security Resource Center, http://csrc.nist.gov/

B.5.3.14 Secure Storage

- Service provider configurable options for securely storing data should be provided. The service provider should be able to specify which fields are stored securely.

B.5.3.16 Software Assurance

Software assurance should be addressed from two perspectives: testing of security features and testing for potential security policy violations.

- Duties must be segregated between software development groups and software testing groups.
- A security test plan, test procedures, and results should be documented.
- All security features must be tested.
- Tests should include attempts to locate violations of security policy (i.e., vulnerabilities such as access control).
- As part of the test, verification must be done so that the newly developed system or application does not introduce vulnerabilities in existing structures, common networks, and systems.
- Verification of secure programming techniques must be performed. Verification may be done via code reviews or software tools.
- All security flaws must be corrected, removed, or neutralized and the system retested.

B.5.3.17 Packaging and Delivery

A software configuration management system must be used throughout the life cycle of a product that maintains control of changes to source code and documentation.

- Developers should not maintain the software configuration management system.
- Developers should not have access to production systems except under controlled emergency provisions that are approved and logged.
- Only authorized code and code modifications should be added to the deliverable source baseline.
- All changes must be documented and reviewed.
- Tools or procedures must exist to generate a new version of the system from source code.
- Tools or procedures must exist to protect the source code from unauthorized modifications.
- Tools or procedures must exist to verify the appropriate versions and levels of component source modules were used.
- The product must contain integrity mechanisms such that it is possible to verify the installed software is consistent with the delivered software (i.e., no unauthorized modifications have been made).
- Where a mechanized scanning tool is available, a vulnerability scan must be completed after upgrades or other significant changes to the OS or application software

- Security flaw remedies or "fixes" must be provided in a timely manner commensurate with the threat.

- A master database must exist that contains copies of all delivered software. The software must have a release number and specifications for appropriate OSs and hardware.

B.5.3.19 Secure Installation, Configuration, and Operation

- Secure configuration parameters should be defined for the software.

- Secure operations procedures should be defined and documented for the software.

- All remote support of the software should be performed in a secure manner.

- All default user IDs delivered with the system should be delivered in an inactive state that requires explicit action by the administrator/software installer to be usable.

- All installation processes should be secure and should not rely on trust relationships (i.e., share drives).

Annex C

(Informative)

C Informative References

This annex includes references that provide additional information on many of the topics addressed in Annexes A and B.

American National Standards Institute (ANSI) J-STD-025 CD, *Lawfully Authorized Electronic Surveillance*, December 2000.

ANSI T1.210-1993 (R1999), *OAM&P—Principles of Functions, Architectures, and Protocols for Telecommunications Management Network Interfaces.*

ANSI T1.233-1993 (R1999), *OAM&P—Security Framework for Telecommunications Management Network Interfaces*.

ANSI T1.243-1995 (R1999), *OAM&P—Baseline Security Requirements for the Telecommunications Management Network*.

ANSI T1.252-1996 (R2002), *OAM&P—Security for the Telecommunications Management Network Directory.*

ANSI T1.261-1998, *Telecommunications—OAM&P—Security for Telecommunications Management Network Management Transactions Over the TMN Q3 Interface.*

ANSI T1.268-2000, *Telecommunications Management Network—Public Key Infrastructure—Digital Certificates and Certificate Revocation Lists Profiles*.

ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*.

ATM Forum. AF-SEC-0179.000 (April 2002), *Methods of Securely Managing ATM Network Elements—Implementation Agreements Version 1.1* (available at ftp://ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).

Barrett, D., and R. Silverman. *SSH, The Secure Shell: The Definitive Guide*. O'Reilly, January 2001.

Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity," *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, April 1995.

Bleichenbacher, D., "Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1," *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, 1998, pp. 1-12.

Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem," *Notices of the American Mathematical Society (AMS)*, Vol. 46, no. 2, February 1999, pp. 203-213 (available at http://www.ams.org/notices/199902/boneh.pdf)

Boneh, D., A. Joux, and P. Nguyen, "Why Textbook RSA and ElGamal Encryption Are Insecure," *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, 2000, pp. 30-43.

Department of Defense Standard 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985, (available at http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html)

Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, September 1999.

General Requirements (GR)-815, *Generic Requirements for Network Element/Network System Security*, March 2002 (available at Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html)

GR-1194, *Bellcore Operations Systems Security Requirements*. December 1998 (available at Telcordia Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html)

GR-2973-CORE (Central Office Relay Equipment), *Lawful Access Feature: Switching Generic Requirements*, April 2000 (available at http://telecom-info.telcordia.com/site-cgi/ido/index.html)

GR-2975-CORE, *Surveillance Administration System Generic Requirements*, September 2000 (available at http://telecom-info.telcordia.com/site-cgi/ido/index.html)

Gutmann, P., “Software Generation of Practically Strong Random Numbers,” *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, 1998, pp. 243-257 (available at http://www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/gutmann.pdf)

Information Assurance Technical Framework Forum (IATF), http://www.commoncriteria.org/ and http://www.iatf.net/protection_profiles/profiles.cfm.

Institute of Electrical and Electronics Engineers (IEEE) 1363-2000, *IEEE Standard Specifications for Public Key Cryptography*. (available at IEEE Standards Online, http://standards.ieee.org/catalog/olis/ busarch.html)

Internet Engineering Task Force (IETF) Request for Comment (RFC) 768, *User Datagram Protocol*, J. Postel, August 1980 (available at http://www.ietf.org/rfc/rfc0768.txt?number=768)

IETF RFC 791, *Internet Protocol*, J. Postel, September 1981 (available at http://www.ietf.org/rfc/ rfc0791.txt?number=791)

IETF RFC 792, *Internet Control Message Protocol*. J. Postel. September 1981 (available at http://www.ietf.org/rfc/rfc0792.txt?number=792)

IETF RFC 793, *Transmission Control Protocol (TCP)*. J. Postel. September 1981 (available at http://www.ietf.org/rfc/rfc0793.txt?number=793)

IETF RFC 826, *An Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*. D. C. Plummer. November 1982 (available at http://www.ietf.org/rfc/rfc0826.txt?number=826)

IETF RFC 859, *Telnet Status Option*. J. Postel, J. K. Reynolds. May 1983 (available at http://www.ietf.org/rfc/rfc0859.txt?number=859)

IETF RFC 959, *File Transfer Protocol*. J. Postel, J. K. Reynolds. October 1985 (available at http://www.ietf.org/rfc/rfc0959.txt?number=959)

IETF RFC 1157, *A Simple Network Management Protocol*. J. Case, M. Fedor, M. L. Schoffstall, J. Davin. May 1990 (available at http://www.ietf.org/rfc/rfc1157.txt?number=1157)

IETF RFC 1288, *The Finger User Information Protocol*. D. Zimmerman. December 1991 (available at http://www.ietf.org/rfc/rfc1288.txt?number=1288)

IETF RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol.* SNMPv2 Working Group, J. Case, K. McCloghrie, M. Rose, S. Waldbusser. January 1996 (available at http://www.ietf.org/rfc/rfc1905.txt?number=1905)

IETF RFC 2045, *Multipurpose Internet Mail Extensions Part One: Format of Internet Message Bodies*, N. Freed and N. Borenstein, November 1996 (available at http://www.ietf.org/rfc/rfc2045.txt?number=2045)

IETF RFC 2202, *Test Cases for HMAC-MD5 and HMAC-SHA-1*. P. Cheng and R. Glenn. September 1997 (available at http://www.ietf.org/rfc/rfc2202.txt?number=2202)

IETF RFC 2222, *Simple Authentication and Security Layer.* J. Myers. October 1997 (available at http://www.ietf.org/rfc/rfc2222.txt?number=2222)

IETF RFC 2246, *The Transport Layer Security Protocol Version 1.0*. T. Dierks and C. Allen. January 1999 (available at http://www.ietf.org/rfc/rfc2246.txt?number=2246)

IETF RFC 2271, *An Architecture for Describing Simple Network Management Protocol Management Frameworks*. D. Harrington, R. Presuhn, B. Wijnen. January 1998 (available at http://www.ietf.org/rfc/rfc2271.txt?number=2271)

IETF RFC 2272, *Message Processing and Dispatching for the Simple Network Management Protocol.* J. Case, D. Harrington, R. Presuhn, B. Wijnen. January 1998 (available at http://www.ietf.org/rfc/rfc2272.txt?number=2272)

IETF RFC 2273, *Simple Network Management Protocol Version 3 Applications*. D. Levi, P. Meyer, B. Stewart. January 1998 (available at http://www.ietf.org/rfc/rfc2273.txt?number=2273)

IETF RFC 2274, *User-based Security Model for Version 3 of the Simple Network Management Protocol.* U. Blumenthal and B. Wijnen. January 1998 (available at http://www.ietf.org/rfc/rfc2274.txt?number=2274)

IETF RFC 2275, *View-based Access Control Model for the Simple Network Management Protocol.* B. Wijnen, R. Presuhn, K. McCloghrie. January 1998 (available at http://www.ietf.org/rfc/rfc2275.txt?number=2275)

IETF RFC 2401, *Security Architecture for the Internet Protocol*, S. Kent and R. Atkinson, November 1998 (available at http://www.ietf.org/rfc/rfc2401.txt?number=2401).

IETF RFC 2402, *Internet Protocol Authentication Header*. S. Kent and R. Atkinson. November 1998 (available at http://www.ietf.org/rfc/rfc2402.txt?number=2402)

IETF RFC 2406, *Internet Protocol Encapsulating Security Payload*. S. Kent and R. Atkinson. November 1998 (available at http://www.ietf.org/rfc/rfc2406.txt?number=2406)

IETF RFC 2451, *The Encapsulating Security Payload CBC-Mode Cipher Algorithms*. R. Pereira and R. Adams. November 1998 (available at http://www.ietf.org/rfc/rfc2451.txt?number=2451)

IETF RFC 2616, *Hypertext Transfer Protocol (HTTP)—HTTP/1.1*, R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. June 1999 (available at http://www.ietf.org/rfc/rfc2616.txt?number=2616)

IETF RFC 2631, *Diffie-Hellman Key Agreement Method*. E. Rescorla. June 1999 (available at http://www.ietf.org/rfc/rfc2631.txt?number=2631)

IETF RFC 3080, *The Blocks Extensible Exchange Protocol (BEEP)Core*. M. Rose. March 2001 (available at http://www.ietf.org/rfc/rfc3080.txt?number=3080)

IETF RFC 3081, *Mapping the BEEP Core onto TCP*. M. Rose. March 2001 (available at http://www.ietf.org/rfc/rfc3081.txt?number=3081)

International Organization for Standardization (ISO) 7498-2:1989, *Information Processing Systems—Open Systems Interconnection Basic Reference Model—Part 2: Security Architecture* (available at ISO Online Store, http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1=35&ICS2=100&ICS3=1)

International Telecommunication Union – Telecommunications Sector (ITU-T) Recommendation M.3010, *Principles for a Telecommunications Management Network*, February 2000, (available at ITU Electronic Bookshop)

ITU-T Recommendation M.3013, *Considerations for a Telecommunications Management Network*, February 2000 (available at ITU Electronic Bookshop)

Jansen, W.A., *A Revised Model for Role Based Access Control*, NIST-IR 6192, July 1998, (available at http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf)

Jonsson, J., and B. Kaliski, "On the Security of RSA Encryption in TLS," *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, August 2002, pp. 127-142.

Kelsey, J., B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator," *Sixth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1999 (available at http://www.counterpane.com/yarrow-notes.html)

Krawczyk, H., "Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol," *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, August 2002, pp. 143-161.

Lenstra, A., and E. Verheul, "Selecting Cryptographic Key Sizes," *Journal of Cryptology*, Vol. 14, no. 4, 2001, pp. 255-293.

National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms.* October 1988 (available at http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf)

National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000 (available at http://www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf)

Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.8.* March 2002, (available at http://cgi.omg.org/docs/formal/02-03-11.pdf)

Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7.* March 2001, (available at http://cgi.omg.org/docs/formal/01-03-08.pdf)

Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, September 2001 (available at http://www.pcis.org/library.cfm?urlSection=WG)

Rescorla, E., *SSL and TLS*, Addison-Wesley, 2001.

Schneier, Bruce., *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996.

Silverman, R., "The Mythical MIPS Year," *IEEE Computer*, August 1999.

Silverman, R., “A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths,” *RSA Laboratories Bulletin*, Number 13, April 2000.

Vaudenay, S., “Security Flaws Induced by CBC Padding—Applications to SSL, IPsec, WTLS,” *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, April-May 2002, pp. 534-545.

World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, February 1998, (available at http://www.w3.org/TR/1998/REC-xml-19980210).

World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, May 2000 (available at http://www.w3.org/TR/SOAP/).

Wu, T., “The Secure Remote Password Protocol,” *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, March 1998, pp. 97-111 (available at http://www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

Ylönen, T., “SSH—Secure Login Connections Over the Internet,” *Sixth USENIX Security Symposium Proceedings*, July 1996, pp. 37-42 (available at http://www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html)