Generic Requirements for Network Element/Network System (NE/NS) Security

A Module of OTGR, FR-439 and LSSGR, FR-64
Generic Requirements for Network Element/Network System (NE/NS) Security

A Module of OTGR, FR-439 and LSSGR, FR-64
This document, GR–815–CORE, Issue 1, November 1997, replaces


For further information, please contact

Ranen Bhattacharyya
(732) 758-5646

For ordering information, see the References section of this document.

This document may not be reproduced without the express written permission of Bellcore and any reproduction without written authorization is an infringement of Bellcore’s copyright.

Copyright © 1997 Bellcore.

All rights reserved.

Project funding year: 1997.
Trademark Acknowledgements

Kerberos is a trademark of the Massachusetts Institute of Technology.

UNIX is a registered trademark of Novell, Inc.
This Generic Requirements document (GR) is published by Bell Communications Research, Inc. (Bellcore) to inform the industry of Bellcore's view of proposed generic requirements. These generic requirements are subject to review and change, and superseding generic requirements regarding this subject may differ from this document. Bellcore reserves the right to revise this document for any reason.

**BELLCORE MAKES NO REPRESENTATION OR WARRANTY, EXPRESSED OR IMPLIED, WITH RESPECT TO THE SUFICCIENCY, ACCURACY, OR UTILITY OF ANY INFORMATION OR OPINION CONTAINED HEREIN. BELLCORE EXPRESSLY ADVISES THAT ANY USE OF OR RELIANCE UPON SAID INFORMATION OR OPINION IS AT THE RISK OF THE USER AND THAT BELLCORE SHALL NOT BE LIABLE FOR ANY DAMAGE OR INJURY INCURRED BY ANY PERSON ARISING OUT OF THE SUFICCIENCY, ACCURACY, OR UTILITY OF ANY INFORMATION OR OPINION CONTAINED HEREIN.**

**LOCAL CONDITIONS MAY GIVE RISE TO A NEED FOR ADDITIONAL PROFESSIONAL INVESTIGATIONS, MODIFICATIONS, OR SAFEGUARDS TO MEET SITE, EQUIPMENT, ENVIRONMENTAL SAFETY OR COMPANY-SPECIFIC REQUIREMENTS. IN NO EVENT IS THIS INFORMATION INTENDED TO REPLACE FEDERAL, STATE, LOCAL, OR OTHER APPLICABLE CODES, LAWS, OR REGULATIONS. SPECIFIC APPLICATIONS WILL CONTAIN VARIABLES UNKNOWN TO OR BEYOND THE CONTROL OF BELLCORE. AS A RESULT, BELLCORE CANNOT WARRANT THAT THE APPLICATION OF THIS INFORMATION WILL PRODUCE THE TECHNICAL RESULT OR SAFETY ORIGINALLY INTENDED.**

This GR is not to be construed as a suggestion to anyone to modify or change any of its products or services, nor does this GR represent any commitment by anyone, including, but not limited to, Bellcore or any funder (see Preface) of this Bellcore GR to purchase, manufacture, or sell, any product with the described characteristics.

Readers are specifically advised that any entity may have needs, specifications, or requirements different from the generic descriptions herein. Therefore, anyone wishing to know any entity’s needs, specifications, or requirements should communicate directly with that entity.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent, whether or not the use of any information herein necessarily employs an invention of any existing or later issued patent.

Bellcore does not herein recommend products, and nothing contained herein is intended as a recommendation of any product to anyone.
Generic Requirements for Network Element/Network System (NE/NS) Security

Contents

Preface ................................................................................................................... Preface–1

1. Introduction ............................................................................................................... 1–1
   1.1 Background ..................................................................................................... 1–1
   1.2 Purpose and Scope .......................................................................................... 1–2
   1.3 Perspective ...................................................................................................... 1–3
   1.4 Intended Audience .......................................................................................... 1–4
   1.5 Terminology .................................................................................................... 1–6
   1.6 Requirements Terminology ............................................................................. 1–8
   1.7 Requirement Labeling Conventions ............................................................... 1–8
       1.7.1 Numbering of Requirement and Related Objects ................................ 1–9
   1.8 Organization of Document .............................................................................. 1–9

2. Rationale for NE/NS Security Measures ............................................................. 2–1
   2.1 NE/NS Threats ................................................................................................ 2–1

3. Security Feature Requirements ............................................................................... 3–1
   3.1 Overview ......................................................................................................... 3–1
   3.2 Identification ................................................................................................. 3–2
   3.3 Authentication ............................................................................................... 3–4
   3.4 System Access Control .................................................................................. 3–8
   3.5 Resource Access Control .............................................................................. 3–12
   3.6 Security Log (Audit) .................................................................................... 3–15
       3.6.1 Security Log Generation .................................................................. 3–15
       3.6.2 Report Generation/Audit Trail ......................................................... 3–17
   3.7 Data and System Integrity ............................................................................. 3–18
       3.7.1 Continuity of Service ....................................................................... 3–20
   3.8 Security Administration ................................................................................ 3–20

4. Development Life Cycle Requirements ............................................................... 4–1
   4.1 Security Policy ............................................................................................... 4–1
   4.2 Requirement Analysis ................................................................................... 4–1
   4.3 System Design ............................................................................................... 4–2
   4.4 Detailed System Design ................................................................................ 4–3
   4.5 Implementation ............................................................................................. 4–3
   4.6 Development Environment ........................................................................... 4–4
   4.7 System Test .................................................................................................... 4–5
   4.8 Packaging and Delivery ................................................................................ 4–6
   4.9 Documentation ............................................................................................... 4–7
4.10 Support ........................................................................................................... 4–8

5. Telecommunications Management Network (TMN) ........................................ 5–1
   5.1 TMN Security ............................................................................................... 5–2
   5.2 TMN Layers for Security Administration .................................................. 5–2
   5.3 Securing the TMN ....................................................................................... 5–2
   5.4 Managing TMN security ............................................................................ 5–3

References ........................................................................................................ References–1

Glossary .............................................................................................................. Glossary–1
Preface

This Preface contains important information about Bellcore’s GR process in general, as well as important information about this document.

Bellcore’s GR Process

Generic Requirements documents (GRs) provide Bellcore’s view of proposed generic criteria for telecommunications equipment, systems, or services, and involve a wide variety of factors, including interoperability, network integrity, funding participant expressed needs, and other input.

Bellcore’s GR process implements Telecommunications Act of 1996 directives relative to the development of industry-wide generic requirements relating to telecommunications equipment, including integral software and customer premises equipment. Pursuant to that Act, Bellcore invites members of the industry to fund and participate in the development process for such GRs. Invitations to fund and participate are issued monthly in the Bellcore Digest of Technical Information, and posted on Bellcore’s web site at http://www.bellcore.com/DIGEST.

At the conclusion of the GR development process, Bellcore publishes the GR, which is available by subscription. The subscription price entitles the purchaser to receive that issue of the GR (GR-CORE) along with any Issues List Report (GR-ILR) and Revisions, if any are released under that GR project. ILRs contain any technical issues that arise during GR development that Bellcore and the funding participants would like further industry interaction on. The ILR may present issues for discussion, with or without proposed resolutions, and may describe proposed resolutions that lead to changes to the GR. Significant changes or additional material may be released as a Revision to the GR-CORE.

Bellcore may also solicit general industry nonproprietary input regarding such GR material at the time of its publication, or through a special Industry Interaction Notice appearing in the Bellcore Digest of Technical Information. While unsolicited comments are welcome, any subsequent work by Bellcore regarding such comments will depend on funding support for such GR work. Bellcore will acknowledge receipt of comments and will provide a status to the submitting company.
About GR–815–CORE

A. Funders of GR–815–CORE, Issue 1, are:

Ameritech, Bell Atlantic, BellSouth, NYNEX, Pacific Bell, Southwestern Bell Telephone, and U S WEST.

B. Relative Maturity Level

This is a mature technology and requirements reflect maintenance mode.

C. GR–815–CORE Plans

There are no current plans to update the material in this GR.

To Submit Comments

When submitting comments, please include the GR document number, and cite any pertinent section and requirement number. In responding to an ILR, please identify the pertinent Issue ID number. Please provide the name and address of the contact person in your company for further discussion.

Comments may be submitted at any time.

Send comments to:

Bellcore — GR–815–CORE
Ranen Bhattacharyya, Project Manager
331 Newman Springs Road, NVC 2X-415
Red Bank, NJ 07701-5699

Phone: (732) 758-5646
1. Introduction

This document proposes Bellcore's view of the generic requirements for Network Elements (NEs) and Network Systems (NSs) security, i.e., the generic security features required of a total NE/NS environment. The document replaces its predecessor, TR-NWT-000815, *Network Element (NE) Memory Administration - Network Element and Network System Security*, Issue 2, published in December 1992.

Switches and Transmission Elements are typical examples of NEs. NSs encompass Adjuncts, Intelligent Peripherals, Gateways, Element Managers, Network Managers¹, etc. Evolving technology and services, in general, tend to accentuate the vulnerability of the NE/NS environment due to the nature of their being new, distributed, and not yet subjected to the tests of time and extensive use. In addition, increasing customer access and involvement of third party service providers open up new points of ingress into the NE/NS environment that require protection against unauthorized access. This document includes Bellcore's view on generic security requirements that are applicable to the evolving NE/NS environments and the associated new technologies. These requirements are generic and are not specific to any particular NE/NS. They provide "baseline" requirements in the sense that they represent minimum expectations in Bellcore's preliminary view. In addition, the NE/NS security requirements are developed with a view to the diverse equipment architectures, network configurations, and service and environments in which the NE/NS has to function.

Adherence to these generic requirements does not guarantee a "secure" system, nor does it alleviate the responsibility for providing and maintaining the NE/NS in a secure fashion. Security is not only the vendor's responsibility but it is also the responsibility of the Bellcore Client Companies (BCCs) and other service providers that use the NE/NS.

1.1 Background

Telecommunications service providers rely on NEs and NSs to provide and support communication services in the public as well as private environments comprised of Circuit Switched Networks, Packet Switched Networks, Cell Switched Networks, Wireless Networks, and Operations Systems Networks. The integrity, availability, and confidentiality of key software systems, databases, and networks are therefore major concerns of all telecommunications service providers. The corruption, destruction, unauthorized disclosure, or theft of communication services and network resources may have a disruptive effect on the service continuity of the public and private network.

---

¹ The "Element Manager" and the "Network Manager" provide management capabilities deployed at the "Element Management Layer" and the "Network Management Layer" respectively, in compliance with the layered architecture introduced by the Telecommunications Management Network (TMN) model. Details of the TMN model are described in Section 5.
environments, as well as serious and immediate impact on national security and financial, legal, and public confidence.

The National Security Telecommunications Advisory Committee (NSTAC) has been concerned with the state of industry endorsed security standards and requirements. To determine the state of security standards, NSTAC created the Network Security Standards Oversight Group (NSSOG) to identify network security issues in the public switched network that could be addressed by additional standards and requirements activity. The NSSOG identified several Public Switched Network (PSN) security standards issues focused on two major areas – policy & procedures, and technology. To categorize the identified issues, the following criteria were used:

- Security standards and requirements need to promote interoperability to get industry acceptance.
- Security standards need to address the risks to network elements, systems, services and applications.
- Security standards should be realistic and capable of being implemented.
- Security standards should cover as broad a range of technologies and architectures as possible.
- Security standards should address issues such as remote access, common access control models, intrusion detection, and emerging technologies (e.g., Broadband).

The security generic requirements described in this document are in conformance with these criteria.

1.2 Purpose and Scope

The generic requirements described in this GR provide baseline requirements from which requirements specific to a particular NE/NS environment may be derived. Baseline requirements define a minimum level of security. Additional security may be needed for specific applications. This baseline is considered to be a starting point and proposed as an input to requirements analysis. It is recognized that the security requirements for a specific application may deviate from the baseline. The baseline is a benchmark with which formal security requirements for a specific application can be compared, with deviations being justified on the basis of considerations such as unique vulnerabilities, associated risks, and sound business decisions. These deviations should be justified, documented, and approved by organizations with appropriate responsibilities.

This document applies to all NEs/NSs manufactured by vendors and used by service providers. In addition, the generic requirements address all phases of the development life cycle and, therefore, apply to both new and existing NEs/NSs. New NEs/NSs need to follow these requirements throughout their life cycle. Existing NEs/NSs need to follow the Development Life Cycle Requirements throughout the remainder of their life cycle.
addition, where technically and economically feasible within the confines of the existing NE/NS architecture, software enhancements that are part of maintenance and new feature releases must follow the *Security Feature Requirements*.

The generic requirements are meant to be used in Technical Analyses (see Glossary) of NEs/NSs at the discretion of vendors and/or service providers. Adherence to these requirements is no guarantee for customer acceptance. The requirements merely provide guidelines against which the security of a product/system may be analyzed.

This document does not address many other aspects of NE/NS security, such as physical security, security awareness training for users, promulgation of effective security management policies and practices among security administrators, etc.

### 1.3 Perspective

This GR replaces TR-NWT-000815 and includes new material so that Bellcore's view on security related generic requirements may keep in step with evolving technologies and services. There are other efforts underway similar to this attempt to define requirements. For example, the National Institute of Standards and Technology (NIST) has published the *Telecommunications Security Guidelines (TSG) for Telecommunications Management Networks (TMN)*.[1] The American National Standards for Telecommunications has issued a security framework (see ANSI T1.233-1993[2]) for interface specifications for various Operations (see ANSI T1.243-1995[3]). It is possible that the Common Criteria,[4] as it matures in the future, may eventually replace the Orange Book.[5] On the international scene, the International Telecommunications Union Telecommunications Standardization Sector (ITUT-T) has published a draft recommendation, M.3400,[6] regarding TMN management functions, which include security management. Bellcore has been a major participant in these national and international efforts and has made contributions such as

- GR-1332-CORE, *Generic Requirements for Data Communication Network Security*[7]
- LP-18, *Analysis of DCE Security*[8]
- GR-1469-CORE, *OTGR Section 15.5: Generic Requirements on Security for OSI-Based Telecommunications Management Network (TMN) Interfaces*[9]

Deployment of new technology, such as Broadband applications, has introduced new dimensions to NE/NS vulnerability. Bellcore has addressed these concerns in documents such as
• GR-253-CORE, *Synchronous Optical Network (SONET): Common Generic Criteria*[^12]

• GR-1327-CORE, *Frame Relay Network Element Operations*[^13]

• GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs).*[^14]

This GR has been influenced by all of the documents referenced here. In addition, this GR is somewhat related to TR-NWT-000835, *OTGR Section 12.5: Operations Application Messages: Network Element (NE) and Network System Security Administration Messages,*[^15] which contains NE/NS security administration messages that correspond to several security administration functionalities described in Section 3.8 of this document.

The generic security requirements described in this GR may be grouped into two broad categories:

1. Generic security feature requirements on NE/NS software products

2. Generic security requirements for software development related to the process-oriented development life cycle.

The two-part nature of the requirements is an important and fundamental aspect in implementing security. Security features and mechanisms are not sufficient by themselves to provide secure NEs/NSs. Features and mechanisms must be properly conceived, designed, implemented, tested, installed, documented, and maintained. Otherwise, a false sense of security may result. The process of providing the software, from beginning to end, has to take security considerations into account. Section 3 presents the generic security feature requirements of NE/NS products, and Section 4 presents the generic security requirements related to the software development life cycle of an NE/NS.

The generic security requirements in this document do not take into account the unique security risks and vulnerabilities of any specific NE/NS, NE/NS configuration, or particular network environment. They are meant to be used as input to the Requirements Analysis phase of the software life cycle, and successively refined and made more specific to the unique risks and vulnerabilities in subsequent phases of the development life cycle of the NE/NS.

### 1.4 Intended Audience

The intended audience for this document consists of three groups:

• NE/NS Developers, i.e., Vendors

• Service Providers deploying NE/NS

• Security Analysts.
The three groups should come to similar conclusions regarding their respective security requirements. For example, when a service provider submits a Request For Proposal (RFP) to a variety of product/system vendors, the RFP can specify this GR as the basis for the security requirements. The vendor can use this GR as the baseline for security requirements to be met by the product/system. The service provider will then be able to call on a third-party analyst to analyze the developed product/system. The security analyst can use this GR to determine the conformance of the said product/system with respect to the baseline requirements.

1. **The NE/NS Developer**

   The vendor needs to assure that the product/system is secure. This implies that security as a feature requirement needs to be addressed by the vendor and integrated in all stages of the life cycle of the product/system, e.g., planning, design, development, maintenance, testing, administration, delivery, etc. This GR can be used by the vendor in all these stages of the NE/NS life cycle to ascertain that the baseline security requirements are met. Depending on the product/system and its deployment, there may be other security-related considerations that the vendor may have to address. These considerations are covered in other Bellcore documents that are more product-oriented and are referenced in this GR when appropriate.

2. **The Service Provider**

   The service provider needs to ensure that the service is secure. All organizations constituting the "service provider" have to take security into consideration, and the list includes organizations such as planning, designing, administration, vendor selection, procurement, maintenance, testing, security audit, etc. These organizations can use this GR to address their respective security concerns.

   During negotiations between the service provider and the vendor, there may be agreement between both parties that not all of the requirements described in this document apply to the product/system in question. The agreement depends on the nature of the product/system, the vulnerability of the environment, and factors such as business considerations. For future reference, the service provider may want to document all deviations (from the generic requirements described in this GR), i.e., the requirements that are deliberately being omitted for the product in question.  

   By documenting the deviation, the requirement is more likely to be addressed if and when the NE/NS environment changes in the future (e.g., a private access to the NE is being replaced by a networked access that may not provide a trusted path).
3. The Security Analyst

The analyst needs a set of criteria for analysis. The generic requirements described in this GR constitute these criteria. The analysis consists of a series of test procedures to determine the conformance and the nonconformance of the NE/NS in question with respect to the generic requirements.

Additionally, the analyst may conduct risk analysis to determine the vulnerability of an NE/NS environment that demonstrates a range of nonconformances. Corresponding to the severity of the risk factor, nonconformances may typically be grouped into three categories: (i) Critical, (ii) Major, and (iii) Minor. As a minimum, the analyst should identify the critical nonconformances as high priority issues to be resolved between the vendor and the service provider.

1.5 Terminology

Throughout this document, several terms are used that carry special connotations. These are explained as follows.

- **Appropriate Administrator**

  An Appropriate Administrator is a highly privileged person who performs security-related administrative tasks. In different organizations, different titles may be used, e.g., System Administrator, Node Administrator, Security Administrator, etc.

- **Class of NE/NS**

  NEs/NSs cover a wide range of products/systems. On the one hand, there are the end-office or tandem switches for large metropolitan and suburban areas. On the other hand, there are products such as broadband (e.g., ATM and Frame Relay) switches and transmission elements such as SONET Add Drop Multiplexers (ADM). The NS may perform any of a wide range of functions related to the NE environment, e.g., (i) TMN-compliant operations functions - as performed by an Element Management System (EMS), (ii) server functions to assist the NE in call handling, (iii) protocol interworking, (iv) information conversion and storage, and (v) management functions for network resources individually or in aggregation as a subnetwork. In order to provide equal protection to all types of NEs/NSs, the total security functionalities ought to be the same for all of them. However, depending on the architecture of the resident and distributed features and the available software processing capabilities, the implementation scheme of the security features may be different in its details. Based on this criterion, NEs/NSs addressed in this GR are divided into two classes.

  1. **Class A** - NEs/NSs belonging to Class A have the capacity to incorporate security parameters in their embedded operating systems and application layers. Examples are large end-office and tandem switches.
2. **Class B** - NEs/NSs belonging to this class have limited software processing capabilities and/or have a distributed management architecture. It may be unrealistic to ask for their security parameters to be embedded within just the NE's operating systems or application layers. The security functions need to be distributed across the NE and the associated NS. The end result has to be that the NE and the NS are protected.

A majority of generic security requirements described in this GR apply to both classes (though details of feature deployment may be different). However, several generic requirements are conditional as to whether the NE/NS belongs to Class A or Class B, and these conditional requirements are clearly stated as such.

- **Customer**
  A customer is a person or organization that is a subscriber to a service offered by a service provider. A *customer* is different from a *user* (See definition of a *user* below.)

- **Port**
  A port of an NE/NS is a point of ingress into the NE/NS. Several of these ports provide Operations, Administration, and Maintenance (OA&M) interfaces. Several others may provide signaling interfaces. Typically, these ports are attached to the NE/NS. However, they may be attached to different types of network nodes and receive their messages and commands from diverse sources, local or remote.

- **Process**
  A process is what an NE/NS invokes to perform the corresponding software-related tasks. The generic security requirements presented in this document apply primarily to those processes that support OA&M tasks. These processes may be initiated by a person or other processes. In addition, several requirements also apply to processes that are associated with the "call-processing" or connection establishment task. For example, an NE/NS may perform access screening when a signaling message is received from another NE/NS.

- **Resources**
  These are software resources of an NE/NS and include such items as data, operational databases, software processes, and communications subsystems. The generic security requirements address protection of various resources in an NE/NS.

- **Requirements**
  See Section 1.6 for the requirements terminology used throughout this GR.

- **User**
  A user is a person, process, or remote system (e.g., OS, NE/NS) in the role of a person, that accesses or attempts to access an NE/NS for the purpose of performing operations-related tasks (e.g., administration tasks, provisioning, maintenance, or testing related to
hardware and software associated with call processing). Thus the concept of a user is different from that of a customer described above.

### 1.6 Requirements Terminology

The following requirements terminology is used throughout this document:

- **Requirement** — Feature or function that, in Bellcore's view, is necessary to satisfy the needs of a typical telecommunications service provider. Failure to meet a requirement may cause application restrictions, result in improper functioning of the product, or hinder operations. A Requirement contains the words shall or must and is flagged by the letter “R.”

- **Conditional Requirement** — Feature or function that, in Bellcore's view, is necessary in specific applications of a service provider and may be reclassified as a requirement by the service provider, depending on the applications environment in which the NE/NS is deployed. Conditional Requirements may depend on other Requirements or Conditional Requirements. A Conditional Requirement is flagged by the letters “CR.”

- **Objective** — Feature or function that, in Bellcore's view, is desirable and may be required by a telecommunications service provider. An Objective represents a goal to be achieved. It may be classified as a Requirement in the future. An objective is flagged by the letter “O” and includes the words it is desirable or it is an objective.

The requirements provide guidelines that can be used to perform a technical analysis of a product/system to determine the level of conformance of its security features. The objectives are not meant to be included in a technical analysis, unless reclassified by a service provider or vendor as a requirement.

When there is a specific relationship between requirements, the first requirement is identified and the subsequent requirement(s) is indented under the first requirement. For example, there are instances where a generic requirement for an NE/NS is followed by a similar requirement (or a conditional requirement) related to whether the NE/NS belongs to Class A or Class B (see definition of "Class of NE/NS" in Section 1.5). The intent is to emphasize that the "high-level" description of a requirement that holds for all NEs/NSs may be enunciated more specifically if the class of the NE/NS is established.

### 1.7 Requirement Labeling Conventions

As part of Bellcore's GR process, proposed requirements and objectives are labeled using conventions that are explained in the following section.
1.7.1 Numbering of Requirement and Related Objects

Each Requirement, Objective, Condition, Conditional Requirement, and Conditional Objective object is identified by both a local and an absolute number. The local number consists of the object's document section number and its sequence number in the section (e.g., **R3-1** is the first Requirement in Section 3). The local number appears in the margin to the left of the Requirement. A Requirement object's local number may change in subsequent issues of a document if other Requirements are added to the section or deleted.

The absolute number is a permanently assigned number that will remain for the life of the Requirement; it will not change with new issues of the document. The absolute number is presented in brackets (e.g., [2]) at the beginning of the requirement text.

Neither the local nor the absolute number of a Conditional Requirement or Conditional Objective depends on the number of the related Condition(s). If there is any ambiguity about which Conditions apply, the specific Condition(s) will be referred to by number in the text of the Conditional Requirement or Conditional Objective.

References to Requirements, Objectives, or Conditions published in other Generic Requirements documents will include both the document number and the Requirement object’s absolute number. For example, **R2345-12** refers to Requirement [12] in GR–2345.

1.8 Organization of Document

The remaining sections of this document are organized as follows:

- **Section 2** - briefly explains the rationale for security controls by describing the threats to the security of NEs/NSs.
- **Section 3** - details the generic NE/NS security requirements for Identification, Authentication, System Access Control, Resource Access Control, Security Log (Audit), Data and System Integrity, and Security Administration.
- **Section 4** - defines the generic requirements for Vendor Development Life Cycle, e.g., various phases of design, development, testing, installation, etc. It also includes requirements related to Packaging, Delivery, and Documentation.
- **Section 5** - describes the security management function in the context of a TMN model that represents a layered architecture of management functions.
- **References** - lists all documents referenced in this GR.
- **Glossary** - lists and defines acronyms and special terms used in this GR.
2. Rationale for NE/NS Security Measures

With advancements in digital technology and software systems, processor-controlled NEs/NSs are proliferating in the network. These NEs/NSs contain databases and different types of software that are accessed and managed by users via different interfaces. New opportunities for services and operations are created. The direct and indirect interfaces to NEs/NSs can be quite varied. For example, a network connection may terminate on an NS which then routes it to an administrative port on the NE. In other configurations, OSs can access the NE/NS via direct links, dial-ups, and data communication networks. However, this connectivity accentuates the security risks of unauthorized access to the NE/NS environment, and its software and databases. Such threats are likely to increase with customers and service providers being given increased access to NE/NS and network services.

2.1 NE/NS Threats

Threat is the possibility of a deliberate or accidental action or condition that may lead to a compromise of security. Unless proper corrective action is taken, the NE/NS may be vulnerable to various threats. Ideally, the implemented NE/NS security features should anticipate and counter all possible threats to the NE/NS and the surrounding network environment. This section articulates and categorizes major known threats, though several of them are outside the scope of this GR.

1. **Type 1** - Confidential information being disclosed via eavesdropping. Examples include

   - Wiretapping messages that may include confidential information such as clear-text passwords. For example, an interloper who is a valid user of a TCP/IP node can execute Source Routing,\(^1\) thus forcing all relevant packets to pass by a surveillance node. In a broadcast mode, packets that are not addressed to the said surveillance node are not supposed to be accepted at that node. However, this difficulty can be circumvented by modifying the software of the node so that ALL packets traveling by the node get accepted.

   - Shoulder-surfing for Charge Card numbers and associated Personal Identification Numbers (PIN).

   - Radio reception of identification numbers of wireless subscribers (e.g., cellular phone users).

---

\(^1\) The Internet Protocol (IP) allows a source to specify a route to a destination and a return path to the origination. Consequently, an interloper may force packets to flow through a specified node where surveillance can be conducted by the interloper.
• Receiving confidential information (e.g., account numbers and passwords) via social engineering.

• Receiving confidential information about customers, users, and system software via "dumpster-diving."

2. Type 2 - Commission of Toll Fraud without tampering with NE operations. Examples include

• Dialing into a Private Branch Exchange (PBX) or CENTREX and then receiving a second dial tone to place a fraudulent call that gets billed to the PBX owner (or the CENTREX subscriber).

• Black Box fraud, committed by a fraudulent PBX owner, by deactivating certain features of the PBX.²

• Fraudulent use of a Voice Mail Box and/or Automated Attendant.³

• Classic toll fraud by using Blue Box, Red Box, etc.⁴

3. Type 3 - Transmit bogus messages over network links and cause service deterioration and/or an intrusion. Examples include

• Access a node in a Common Channel Signaling (CCS) network and transmit bogus Signaling System 7 (SS7) messages to create network congestion and service deterioration.

• Perform "Address Spoofing." Spoofing (also called masquerading) implies that an entity pretends to be another entity to accomplish unauthorized access, execute unauthorized functions, etc.

4. Type 4 - Intrusion into Operations and controlling the NE/NS. Examples include

• Disclosure of information: Confidential data, such as from a Service Control Point (SCP), may be retrieved without authorization and disclosed/sold.

• Unauthorized Provisioning: Unauthorized access into a provisioning channel of a switch can be made to create unauthorized Directory Numbers and services. By the same token, authorized DNs and services may be deleted to create denial of authorized service.

---

² Black Box fraud is characterized by the alteration of a Customer Premises Equipment (CPE) in such a way that a call can be successfully completed to the CPE without the generation of an associated billing. Depending on the switch from where a call is placed to the PBX, billing can be avoided if certain features of the PBX are deactivated.

³ This example refers to intrusion via the signaling channels. It does not include intrusion into the operations of the Voice Mail (which is categorized as a Type 4 event).

⁴ Commission of this type of fraud requires in-band signaling. It does not work for Common Channel Signaling (CCS).
• Unauthorized Modification/Destruction of NE/NS Resources: This includes modification of software and translations, inserting bugs, viruses, and trojan horses, disabling audit trails, and crashing the NEs/NSs.

It should be mentioned that not all threats are posed by outside intruders or malicious "insiders." A security compromise may also be accidentally caused by unsuspecting insiders. There is a need to protect the NE/NS from these threats. To provide adequate protection to a specified NE/NS, it is essential to define the perimeter of the said NE/NS. Depending on the application and its network connectivities, the perimeter may include NEs and NSs of various shapes and sizes, e.g., from an isolated switch to a complex system consisting of ADMs, EMSs, and Network Management Systems (NMSs). Once the perimeter of a given NE/NS is defined, the generic security feature requirements will apply for the system bound within that perimeter.
3. Security Feature Requirements

3.1 Overview

NE/NS security feature requirements can be categorized as follows:

1. Identification

Identification is the process of recognizing a session requester's unambiguous and auditable identity, such as a user-ID. It is a "name" by which a valid user is recognized by the NE/NS without any ambiguity. The user-ID need not be confidential.

2. Authentication

Authentication is the process of verifying the claimed identity of the session requester. For example, a password check, dial/dial-back, Automatic Number Identification (ANI), or smart card validation can serve as the process for this verification. With the advent of new technology, other forms of authentication, at various stages of success, are becoming available, such as voice recognition, handwriting recognition, retina scan, etc.

3. System Access Control

System Access Control authorizes establishment of a session (i.e., login) and continuation of a session until logoff. System access is allowed only to those users that are identified and authenticated.

4. Resource Access Control

Resource Access Control provides the capability of denying access to the NE/NS resources in the absence of proper authorization (e.g., user privilege, channel privilege, etc.). Whether to allow or deny access to a certain resource depends, in general, on factors such as the nature of the resource, the user-ID requesting the access, the point of origination of that request, the input channel over which the request arrives at the NE/NS, etc. In addition, the access permission may depend on several other factors such as

- The command associated with the access, e.g., read, write, execute, etc. A user may be allowed the permission to read, but not to write.

- The resource identifier, e.g., the record which is being accessed. For example, a provisioning craftsperson may have the permission to "write" on a "subscriber line

---

1. There may be situations where a user may have more than one user-ID. Also, there may be cases where a group of users may share a common user-ID. Hence a user-ID need not be a unique attribute of a user. However, given a user-ID, the NE/NS needs to have the capability to identify the corresponding user (or the group of users) without any ambiguity.
translation," but may not have the "read" permission for a file containing passwords.

- The resource attribute, e.g., the field of the record in question that is being accessed. For example, a craftsperson may have the permission to access the record corresponding to a specified DN in a subscriber loop table and write on a field that specifies the class feature of that DN, but the same craftsperson may not have the permission to write on some other field of the same DN record that specifies the usage details (which are used for billing) of that DN.

An example of resource control is to restrict a user from executing an unauthorized command which, in the case of Transaction Language 1 (TL1), includes attributes such as the command verb, the modifiers, the staging parameters, and the data parameters. Permission or denial to execute a command may be conditional on any of these attributes. A point should be made that resource access control is not conditional upon the usage of TL1. Depending on the architecture of the NE/NS resources and the structure of commands for accessing them, resource control functionalities may be packaged differently.

5. Security Log (Audit)

Security log provides tools to establish an audit trail. If a security breach is suspected, an audit trail may be used to investigate whether/how the breach has occurred.

6. Data and System Integrity

Data and system integrity deals with consistency and reliability issues associated with the NE/NS system and its data and software resources. It also includes being able to maintain an acceptable level of service if and when a security intrusion occurs.

7. Security Administration

Security administration consists of proper activation, maintenance, and usage of the security features of an NE/NS, conducted by an appropriate administrator. It includes, among other functions, overriding vendor-supplied defaults, ensuring appropriate backup procedures, "managing" the security database (i.e., keeping up to date the data that represent security parameters), and generating security audits when needed.

3.2 Identification

A user may be a person, a process, or some other system (e.g., an OS, another NE/NS) that accesses or attempts to access the NE/NS to perform operations-related tasks or process a call.

---

2. TL1 is a language developed by Bellcore, primarily for OS-to-NE/NS interfaces, and is based on the syntax of CCITT/Man Machine Language (MML).
R3-1 [1] All authorized users shall have unambiguous user-IDs for identification purposes to support individual accountability, auditability, and access privilege.

R3-2 [2] The NE/NS shall support the unambiguity of a user-ID. This implies that the NE/NS shall not allow an appropriate administrator to create (e.g., by mistake) a user-ID that already exists.

R3-3 [3] At any given instance of time, the NE/NS shall internally maintain the identity of all user-IDs logged on at that time.

R3-4 [4] A process, related to NE/NS operations, that is invoked by a user, shall be associated with the user-ID of that user. This user may be a person, a system such as an OS, another process, etc. For a process invoked by another process (which may have been invoked by a user), the invoked process shall be associated with the ID of the invoking process. Autonomous processes (i.e., processes running without user invocation, such as print spoolers, database management servers, translation process monitors, etc.) shall be associated with an identification code (e.g., "system ownership").

CR3-5 [5] An NE/NS belonging to Class A shall have the capability to disable (as distinct from deleting) a user-ID after a specified time interval, if that user-ID has never been used during that time interval. This capability shall be either an autonomous disabling of the user-ID by the NE/NS, or an alarm/alert generated by the NE/NS for an appropriate administrator who then, depending on the policy, may disable the user-ID by using appropriate commands.

R3-6 [6] The default time interval shall be between 45 and 90 days for disabling a user-ID that has not been used during that time interval.

O3-7 [7] An NE/NS belonging to Class A should support temporary disabling of user-IDs (e.g., based on holidays in a year, days of the week, hours of the day).

O3-8 [8] The mechanism that disables user-IDs should provide an option for automatic reactivation.
3.3 Authentication

The NE/NS shall verify the "claimed identity" of a session requester with the help of an "authenticator." The "authenticator" is some entity that is associated with the "claimed identity" (e.g., a piece of confidential information, a personal attribute, a private possession, etc.), which is assumed to be not duplicable by a masquerader. Traditionally, this authenticator has been the password. However, it can take other forms, such as a Personal Identification Number (PIN), biometric parameters (hand print, voice print, retina scan, etc.), a smart card type login, zero base knowledge (such as random questions of a personal nature that an intruder is not likely to answer correctly), trusted third party authentication, public/private key technology, etc.

Highly sophisticated and easy-to-use (PC-compatible) password cracking devices, packaged in various names and forms, are becoming readily available on the market. As such, passwords are becoming less and less effective in providing adequate security. This is especially true for remote logins (e.g., network access, dial-in), where passwords are transmitted over links that may be tapped. Consequently, if a password is used to authenticate a remote login, it is required that the process of authentication be enhanced by using an additional or more sophisticated authenticator. Depending on the application, there are different ways to perform this "enhanced authentication," as follows:

- Smart cards may provide a convenient and effective means to enhance authentication for a wide range of applications.
- For dial-up channels, security can be improved by a dial/dial-back mechanism.
- For network access channels that use a three-layer protocol (for example, X.25), network-level security (though it does not guarantee end-to-end connection security) may be provided by verifying the calling address that is delivered to the NE/NS via the "call set-up packet."
- Authentication can be enhanced by employing trusted third party authenticators (e.g., Kerberos™), one-time authentication schemes, public/private key technology, etc.

R3-9 [9] The NE/NS shall have the capability to verify the claimed identity of a session requester with the help of the authenticator(s) provided by the said session requester.

R3-10 [10] The NE/NS shall not support ways to bypass the deployed authentication mechanism.

Under either of the following conditions, the NE/NS shall have the capability to perform enhanced authentication,\(^3\) i.e., authentication beyond a password verification:

\[
\begin{align*}
\text{1.} & \quad \text{The NE/NS allows remote sessions (which may be established over public or shared networks).} \\
\text{2.} & \quad \text{The NE/NS has users authorized to perform functions deemed critical beyond a password protection.}
\end{align*}
\]

In addition to the above, if the authenticator is a password, the following generic requirements hold:

\[
\begin{align*}
R3-13 & \quad \text{The NE/NS shall not prevent a user from choosing (e.g., unknowingly) a password that is already associated with another user-ID. (Otherwise, an existing password may be divulged.)} \\
R3-14 & \quad \text{The NE/NS shall store passwords in a one-way encrypted form.} \\
R3-15 & \quad \text{The NE/NS shall not store or retain any clear text password in any location. An occurrence of a clear text password in the memory (e.g., during login) shall be overwritten immediately after its use.} \\
R3-16 & \quad \text{The NE/NS shall automatically suppress or blot out the clear text representation of a password on the data entry device.} \\
R3-17 & \quad \text{Passwords in clear text shall not be available to any user, including appropriate administrators. An appropriate administrator may be allowed to retrieve encrypted passwords.}\(^4\) \text{ However, encrypted passwords shall not be available to any other user.} \\
R3-18 & \quad \text{The NE/NS shall provide a mechanism for a password to be user changeable. This mechanism shall require reauthentication of user identity.}
\end{align*}
\]

\(^3\) Depending on the application, enhanced authentication may be performed in several ways, as described earlier. In the case of an NE belonging to Class B which may not possess the processing power to perform enhanced authentication, the totality of the NE/NS architecture shall provide enhanced authentication for remote logins and critical transactions.

\(^4\) It is recognized that, depending on the NE/NS environment, it may not be realistic to make the encrypted password file unavailable to an appropriate administrator. However, it is recommended that this capability of the appropriate administrator be curtailed to the extent it is feasible, by employing techniques such as hashing the bytes of an encrypted password in a proprietary way.
R3-19 [19] After a password is assigned to a human user, when that user establishes a session for the first time, the NE/NS shall prompt the user to change the password and deny the session if the user does not comply.

R3-20 [20] The NE/NS shall enforce password aging (i.e., a password is required to be changed after a specified interval).

R3-21 [21] The default⁵ for the system-wide password aging interval shall be between 20 and 90 days.

CR3-22 [22] If the following conditions hold, the NE/NS shall provide the capability to set the password aging interval on a "per user-ID" basis:

… 1. The NE/NS supports privileged users (such as "superusers" in a UNIX® environment), i.e., users that are allowed additional data, transactions, or service access.

… 2. The NE/NS supports machines⁶ (e.g., remote OS) as users.

CR3-23 [23] An NE/NS belonging to Class A shall provide a mechanism to notify users in advance to change their passwords upon expiration. Two ways of doing this are as follows:

… 1. The user is notified a specified period of time before the password expiration. The default for the specified time period shall not be greater than 7 days.

… 2. The user is notified upon password expiration, but allowed a specified additional number of subsequent logins before requiring a new password. The default for the number of subsequent logins shall not be greater than three.

R3-24 [24] For a user updating a password, there shall be a specified minimum period of waiting before an existing password can be updated (except for the first time update, which is required to be performed when the user logs in for the first time after being assigned a password), and the NE/NS shall not allow the reuse of a specified number of most recently used passwords. This requirement discourages password "flipping."

⁵ An appropriate administrator shall have the capability to override this system-wide default with some other value, if desired.

⁶ A remote OS may, on a continuous basis, be logged on to the NE/NS. If, due to some unforeseen reason such as a power failure, the session is interrupted, an expired password may be a hindrance to re-establishing the session, especially if the OS is not always attended by human users. As such, a relatively long password aging interval may be desirable for the OS.
R3-25 [25] The default for the minimum waiting period shall be 20 days, and the default for the specified number of most recently used passwords not allowed to be reused shall be five.

R3-26 [26] A user-entered password shall meet the following complexity requirements (so it cannot be "easily guessable"): …

1. A user-entered password shall contain a combination of at least six alphanumeric characters, including at least one alphabetic, one numeric, and one special (e.g., punctuation) character.

…

2. User-entered passwords shall not contain the associated user-ID.

CR3-27[27] If the NE/NS does not distinguish between upper- and lower-case alphabetic characters, the minimum acceptable length of a user-entered password shall be eight characters (instead of six mentioned above).

O3-28 [28] For user-entered passwords, the password complexity checking algorithm should be modifiable by site. (These modifications do not necessarily imply a change in the "logic" of the algorithm, but rather to its data parameters.)

O3-29 [29] The NE/NS should provide a mechanism to prevent a user from selecting a password from a specified set of excluded passwords, such as locally used acronyms, surnames, etc.

R3-30 [30] If passwords are generated by the NE/NS, the NE/NS-supplied passwords shall meet the following requirements: …

1. NE/NS-supplied passwords shall be "reasonably" resistant to brute-force password guessing attacks, i.e., the total number of NE/NS-generated passwords shall be on the same order of magnitude as what a user could generate using the rules specified for user-entered passwords.

…

2. The generated sequence of passwords shall have the property of randomness, i.e., consecutive instances shall be uncorrelated, and the sequence shall not display periodicity.

CR3-31[31] For NE/NS-supplied passwords, if the "alphabet" used by the password-generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.

---

7. It is recognized that the selection among special characters may be limited by the fact that several of them may have global interpretations; this excludes them from being used as characters for passwords.
O3-32  [32] For *NE/NS-supplied* passwords, the password-generation algorithm should generate passwords that are easy to remember, i.e., pronounceable or paraphrases. (Otherwise a human user may be prone to jot it down, possibly in a prominently visible way.)

### 3.4 System Access Control

The system access control mechanism deals with security features associated with system access for establishing and continuing a session. Before granting a session, the NE/NS has to validate and authenticate the session requester. Validation implies confirming that the user-ID is legitimate. Authentication implies performing a password check and checking other attributes that constitute enhanced authentication. In addition, the NE/NS also needs to ensure that the communication path between the NE/NS and the session requester is trusted so that no intruder can enter the channel. A dedicated cable that is physically secure and not exposed to outsiders may qualify as a trusted path. In other situations, enhanced authentication consisting of additional verification may be needed to keep intruders away. This enhanced authentication may take one of several forms, such as may be provided by dial/dial-back, smart card type login, selective call acceptance when calling number (or ANI) is available to the NE/NS, verification of data entry device, trusted third party authentication, use of public/private key technology, etc. The objective is to reduce the risk of unauthorized access to the NE/NS.

R3-33  [33] The NE/NS shall not allow system access to any user unless identified and authenticated. Only authorized users shall be allowed system access. This holds for all users (i.e., persons, processes, or remote systems).

CR3-34[34] Depending on the application, i.e., if the NE/NS offers a remote login feature (e.g., over public or shared data networks), it shall not grant a remote login without performing enhanced authentication of the session requester.

R3-35  [35] All ports of the NE/NS that accept operations-related command inputs shall exercise system access control. This includes ports that provide direct access, dial-up access, access via a wireless channel, network access, and access via a Data Communications Channel (DCC) as in the case of an Add Drop Multiplexer (ADM) in a Synchronous Optical Network (SONET).  

---

8. For an NE (such as one belonging to *Class B*) which may not have the capability to exercise system access control for a port that provides a network access or a DCC access, the totality of the NE/NS configuration has to provide the required system access control. In the case SONET application, this may require installation of a firewall to deny a DCC access over an administrative boundary.
CR3-36[36] Depending on the application, i.e., if the NE/NS is to be accessed by users and customers who need to keep this access (including the fact that an access is being made) confidential from other customers and users such as unauthorized telephone company employees, the NE/NS shall provide a separate port for such confidential access and shall ensure that messages (including login requests) at this "special" port are kept confidential from users logged on at other ports.

CR3-37[37] If the following conditions hold, the NE/NS shall have the capability to deny system access to all session requests (i.e., disable the points of ingress) in response to appropriate messages received from a central controller such as an EMS:

1. The NE/NS belongs to Class B.

2. The NE/NS is deployed with such numerosity (e.g., SONET ADMs) that turning off all points of ingress on an individual NE basis is unrealistic.

CR3-38[38] Depending on the application, i.e., if the NE/NS provides an emergency entry port without system access control, the NE/NS shall generate a real-time alarm/alert when this port is used to gain access to the NE/NS.

CR3-39[39] Depending on the application, i.e., if the NE/NS provides an emergency entry port without system access control, that port shall recognize only those commands that perform system restoration (for example, from a disk) and no other operations commands.

R3-40 [40] The NE/NS shall not allow any session to be established via a port that is not designed to accept operations-related command inputs. For example, if the output port receives a login request, the NE/NS shall not respond.

R3-41 [41] The NE/NS shall not provide any mechanism to "null" a password. No user-ID shall be allowed unauthenticated system access. Under special situations, such as during installation of a new NE/NS or a new generic software in an existing NE/NS, a default user-ID may be used temporarily, but that default ID shall be associated with a password (typically agreed on

9. This requirement refers to a situation where sensitive switch-based information needs to be confidentially retrieved by an appropriately authorized agency under a court order.

10. Also referred to as the Emergency Action Interface (EAI).
between the BCC and the vendor), which shall be modifiable by an appropriate administrator at any time during the installation processes.

R3-42 [42] The NE/NS shall perform the entire user authentication procedure even if the user-ID that is entered is not valid.

R3-43 [43] The error feedback generated by the NE/NS after the user authentication procedure shall provide no information other than "invalid," i.e., it shall not reveal which part of the user-entered information (user-ID and/or authenticator) is incorrect.

R3-44 [44] The NE/NS login procedure shall exit and end the attempted session if the user-entered information is incorrect, up to a specified number of times.

R3-45 [45] The default for the specified number of times that the NE/NS login procedure shall exit and end the session (due to incorrect user entered information) shall be between two and five (inclusive of both).

R3-46 [46] The NE/NS shall provide a mechanism to immediately notify (in real time) an appropriate administrator when the threshold for incorrect user-entered information is exceeded.

R3-47 [47] When the threshold for incorrect user-entered information has been exceeded, the NE/NS shall lock out the channel (i.e., no login process can be restarted on the same port) for a specified interval of time. The objective is to interrupt the progress of a mechanized password-cracking algorithm.

R3-48 [48] The default for the lock-out duration shall not be longer than 60 seconds when the threshold for incorrect user-entered information has been exceeded. (This is because longer delays can be used to temporarily disrupt the service by systematically locking out all input ports.)

R3-49 [49] The NE/NS shall allow the lock-out duration to be assignable, so there shall be provision for an appropriate administrator to lock the channel out for durations different from the default setting, including an indefinite lock-out until unlocked by the administrator.

R3-50 [50] When the threshold for incorrect user-entered information has been exceeded, the NE/NS shall not, as a default arrangement, suspend the associated user-ID. (This is because suspension of user-IDs can be used to systematically disable all user-IDs.)
R3-51 [51] After a successful login has occurred but before system access is granted, the NE/NS shall provide an advisory warning message regarding unauthorized entry/use and its possible consequences. A warning message is a standard feature for computing environments to explicitly warn intruders and, in certain states, may be a prerequisite to prosecuting them.

R3-52 [52] The advisory warning message at the point of entry to the NE/NS shall be specifiable to meet local requirements and state laws.

R3-53 [53] At the first point of entry, the NE/NS shall have the capability to display a warning message of up to 20 lines in length.

R3-54 [54] As part of delivered software, an appropriate default message shall be provided that warns against unauthorized access or use. As an illustration, the default message may be as follows:

**NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.**

CR3-55 [55] If the NE/NS belongs to Class A, the following shall be displayed upon successful access to the NE/NS:

… 1. The date and time (and location identifier, when available) of the user's last successful access to the NE/NS.

… 2. The number of unsuccessful attempts by that user-ID to gain system access to the NE/NS (e.g., mistyped password) since the last successful access by that user-ID.

R3-56 [56] The NE/NS shall provide a time-out feature. This implies that, if during a session, there has not been any exchange of messages over a channel for a specified period of time, the NE/NS shall lock out that channel for subsequent inputs\(^\text{11}\) (or re-authenticate user before accepting subsequent inputs).

R3-57 [57] The default for the time-out interval shall be between 10 and 30 minutes.

R3-58 [58] The NE/NS shall provide a mechanism for user-initiated keyboard locking. When a keyboard is locked, the channel time-out feature shall be suspended. The unlocking of a locked keyboard shall require

---

11. The NE/NS may not refrain from transmitting outputs over a timed-out channel. This is to allow functions such as retrieval of delayed responses, generation of delayed reports, etc.
authentication (e.g., entering the password). When the keyboard is unlocked, the channel time-out feature shall be resumed.

**R3-59** [59] The NE/NS shall provide a mechanism to end a session through a secure logoff procedure. This implies that when a user terminates a session by logging off, the NE/NS shall ensure that the port drops immediately and the processes running at the time of logoff are terminated. When a subsequent user attempts to log on to that port, the user shall be required to go through the entire login procedure including identification and authentication, and shall not be granted automatic access (i.e., bypassing the login procedure) to any process invoked by the previous user.

**R3-60** [60] The NE/NS shall drop a port immediately if a session is interrupted due to reasons such as time-out, power failure, link disconnection, etc., and the same login procedure as described above shall be required of a subsequent session request.

**CR3-61** [61] Depending on the application, i.e., if the NE/NS employs external modems to perform dial/dial-back, the corresponding modems shall have the following characteristics:

- 1. The modem, after receiving a call from a session requester, shall disconnect the line before dialing the authorized number to re-establish the contact. Additionally, the dial-back shall be performed over a line different from the line over which the session request arrived at the modem.

- 2. A loss of power to the modem shall not cause the modem to fall back to a default password.

- 3. The password file in the modem shall not be readable by a user.

- 4. The modem shall prevent any modification of its stored configuration unless the user attempting this modification is properly authenticated and found to be authorized for this action.

**O3-62** [62] The NE/NS should provide a mechanism to include or exclude users and channels based on parameters such as time-of-day, day-of-week, calendar date, and location of entry.

### 3.5 Resource Access Control

The resource access control feature deals with restricting the usage of the NE/NS resources (process, command, database, etc.) on a "minimum privilege principle." Various levels of privileges (i.e., levels of access permissions) may be assigned to users, data entry devices,
and NE/NS ports for restricting the usage of NE/NS resources. These levels may have to be determined on the basis of the type of process to be executed, the type of resource to be accessed, and the type of function such as Create, Retrieve, Update, or Delete (referred to as "CRUD" functions) to be performed. The NE/NS has to provide features such that these privileges can be assigned in a way that limits access to only those levels that are needed to perform the job function. A few examples of such features are as follows:

1. Command Control: This is accomplished by assigning command execution privileges to user-IDs, data entry devices, input ports, etc. These privileges determine the respective command sets that are authorized for them (e.g., a given user-ID may be authorized to read a given table but not edit the table). For a given session, the NE/NS determines the lowest common denominator (i.e., the intersection) of the authorized command sets and allows execution of only those commands during that session.

2. Object Control: This deals with privileges which, for an object (e.g., a data file/table), specify the user-IDs, data entry devices, input ports, etc. that are authorized to access the said object.

3. Record Control: Since a record in a data table can be conceived of as a row in that table, record control requires a finer granularity than object control. Record control is especially relevant for customers and third party service providers who control their services and networks by accessing the same data tables (but different records) in the NE/NS. The records that are proprietary for a customer must be protected from access by all other customers and enhanced service providers that are not authorized to do so.

4. Field Control: Since a field within a certain record is an attribute of that record, a field can be conceived of as a column of a data table (i.e., part of an object) that the said record belongs to. As such, field control requires a finer granularity than object control.

An alternative approach to accomplish field control is to define different commands to perform the same function on different sets of fields, and then to implement appropriate command control. However, this approach may create command proliferation.

R3-63 [63] The NE/NS shall not allow resource access to any user who has not established a system access (i.e., a login with identification and authentication). This holds for all users (i.e., persons, processes, or remote systems).

R3-64 [64] Subsequent to granting a system access to a user, the NE/NS shall not allow the user to access a resource unless that user-ID has an appropriate privilege to access that resource.

12. A record is also referred to as an "object instance."

13. A field is also referred to as an "attribute."
R3-65 [65] Assigning passwords to specific actions (e.g., operations-related commands) shall not be used as a primary access control method (though it may be used to augment access control). If such a password is assigned, it loses its confidentiality because it has to be shared among all authorized users.

O3-66 [66] A scheme such as a Secure Digital Signature should be used to augment access control, especially for applications where CRUD functions are performed from a remote location on sensitive NE/NS software and data.

CR3-67 [67] Depending on the application, i.e., if the NE/NS is to be accessed by users and customers (including third party service providers) who need confidentiality of their respective resources (which may contain proprietary or classified information) from one another or from unauthorized telephone company personnel, the NE/NS shall provide that confidentiality by protecting one user’s resource from being accessed by others who do not have such authorization.

CR3-68 [68] Depending on the application, i.e., if new resources are created, access to newly created resources shall, by default, be limited in conformance with the privilege(s) of the creator of the resource.

CR3-69 [69] If the application requires the NE/NS to provide different channels/ports for different functions, access to NE/NS resources over a given channel/port shall be controlled on the basis of privileges assigned to that channel/port.

R3-70 [70] The NE/NS shall provide a level of granularity such that, for any specified resource controlled by the NE/NS, it shall be possible to

14. A Secure Digital Signature typically consists of a private key encryption of a hashed representation of a message, which is transmitted along with the message. The receiver decrypts the signature using a public key and, additionally, hashes the message. If the decrypted signature and the hashed message are identical, the identity of the user transmitting the message, as well as the integrity of the message, are confirmed.

15. If resource control mechanisms such as command control, object control, record control, and field control fail to provide the required confidentiality, it may be necessary to partition the NE/NS database to protect one user's data from being accessed by another.

16. For example, a "Delayed Print" command shall not print a file for a user who is not authorized to print that file under the normal print command.

17. A specified resource may include a process, a command, a data table, a record of a data table, a field of a record, etc. The idea is that the resource control needs to be customizable by an appropriate administrator. The structure must not be hard coded in the NE/NS.
... 1. Grant access rights to a specified user or a group of users
... 2. Deny access rights to a specified user or a group of users
... 3. Grant access rights to a specified channel/port or a group of channels/ports
... 4. Deny access rights to a specified channel/port or a group of channels/ports.

R3-71 [71] The NE/NS shall provide adequate granularity to deny a user access to potentially damaging processes and transactions that the user does not have to access to be functional.

R3-72 [72] The NE/NS shall provide adequate granularity to deny a channel/port access to potentially damaging processes and transactions that the channel/port does not have to access to be functional.

R3-73 [73] The NE/NS shall provide adequate granularity to deny a user (as well as a channel/port) access to data files and/or tables unless the user (as well as the channel/port) is authorized for it.

CR3-74[74] Depending on the application (i.e., if the NE/NS has its operations database structured on the basis of commands, views, records, and fields), the NE/NS shall provide adequate granularity to restrict, on the basis of user-ID as well as channel/port, the execution of any specifiable command on any specifiable view, record, or field.

3.6 Security Log (Audit)

The security log (audit) feature provides adequate capabilities to investigate unauthorized activities after they occur so that proper remedial action can be taken. Typically, this implies generating security logs and generating reports to establish audit trails.

3.6.1 Security Log Generation

R3-75 [75] The NE/NS shall generate a security log that contains information to support after-the-fact investigation of loss or impropriety and appropriate management response.

R3-76 [76] Security log entry of any request or activity that is invoked by a user-ID shall include that user-ID, so it becomes possible to establish user
accountability. The term "user-ID" has to be interpreted in a broad sense to include users as well as processes, as described in R3-4.

**CR3-77** Depending on the application, i.e., if the NE/NS accesses other systems to pass on a request or activity that has a user-ID associated with it, the NE/NS shall have the capability to make that user-ID available to other systems. Thus, if the other systems have the capability to accept the user-ID information, the said user can be traceable for the lifetime of the request or activity.

**R3-78** The security log shall be protected from unauthorized access or destruction. The protection shall be provided by access control based on user and channel privilege.

**R3-79** The NE/NS shall not provide any mechanism for any user, including an appropriate administrator, to modify or delete a security log.

**R3-80** The security log shall have a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest), and an appropriate administrator shall have the capability to retrieve, print, copy, and upload the security log (typically to some OS or some other facility for long-term storage).

**R3-81** The NE/NS shall support the capability to specify the condition (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload) that necessitates uploading the security log (typically to some OS or other facility for long-term storage) to avoid an overwrite in the buffer. This upload may be automatically performed by the NE/NS, or by an appropriate administrator if the NE/NS generates an alarm/alert.

**R3-82** When the security log is copied to other media or locations, the copy shall maintain time sequentially and include all records stored in the log up to the time when the copying starts.

**R3-83** The security log and its control mechanisms shall survive system restarts (e.g., via reloading).

**R3-84** The security log, by default, shall record at least the following events:

- 1. Invalid user authentication attempts (equivalently, alarms/alerts generated due to invalid authentication attempts)
- 2. Unauthorized attempts to access resources (e.g., data, transactions, and processes)
3. Changes made in a user's security profiles and attributes

4. Changes made in security profiles and attributes associated with a channel/port

5. Changes made in access rights associated with resources (i.e., privileges required of a user and a channel/port to access a resource)

6. Changes made in the NE/NS security configuration

7. Creation and modification of NE/NS resources performed via standard operations and maintenance procedures. (This does not address creations and modifications carried out on an "offline" basis.)

CR3-85 [85] Depending on the applications (i.e., the two conditions stated below), the security log shall record at least the events included therein

1. If the NE/NS supports privileged users (such as "superusers" in a UNIX environment), logins and activities of privileged users

2. If the NE/NS contains resources deemed to be critical (for example, via risk analysis), authorized access to those critical resources.

R3-86 [86] For each recorded event, the record in the security log shall include at least the following:

1. Date and time of event

2. User identification including associated terminal, port, network address, or communication device

3. Type of event

4. Names of resources accessed

5. Success or failure of the event.

R3-87 [87] The NE/NS shall provide a mechanism to immediately notify, in real time, an appropriate administrator (e.g., via alarm, alert, online report) if the security log fails to record the events that are required to be recorded.

R3-88 [88] Actual or attempted passwords shall not be recorded in the security log.

### 3.6.2 Report Generation/Audit Trail

The report generation/audit trail feature is related to a "post mortem" (i.e., after the event) analysis to investigate any security breach suspected to have occurred.
R3-89 [89] The NE/NS shall provide post-collection audit analysis tools that can produce typical reports (e.g., exception reports, summary reports, detailed reports) on specific data items, users, or communication facilities.

O3-90 [90] The NE/NS should have the capability to monitor, in real time, the occurrence or accumulation of security auditable events that may indicate an immediate security violation. When predefined thresholds are exceeded, the NE/NS should immediately notify an appropriate administrator. If the occurrence or accumulation of the security-related events continues, the NE/NS should take the least disruptive action to terminate the event.

3.7 Data and System Integrity

Security is a vital part of data and system integrity. Integrity includes not only consistency and reliability of the NE/NS system and data, but also the issues related to providing an acceptable level of service. Integrity of data has to be ensured during processing, storage, and transmission/reception of data. When a service degradation occurs, a question arises as to whether the degradation is due to a security compromise or some other factor (such as an overload, integrity failure, etc.), and the security compromise need not involve intrusion into an operations channel of the NE/NS.18 To answer the question, there is a need to analyze the trend in service deterioration and incorporate adequate reporting functions.

R3-91 [91] For user-accessible resources in the NE/NS that are created or modified by a user-ID19 via standard operations and maintenance procedures, the NE/NS shall provide a mechanism to identify the said user-ID, date, and time associated with the said resource creation or modification.

O3-92 [92] Error detection protocols should be used when sending information across communications channels.

O3-93 [93] When information is of a sensitive or private nature, consideration should be given to utilizing data encryption (and partitioning of the databases, if required) to preserve the confidentiality of the information.

18. For example, an intruder may cause service deterioration by injecting bogus signals in the network. An interloper may commit toll fraud in one of various ways without getting into the operations channel of an NE/NS.

19. The word user-ID is to be interpreted in a broad sense to include persons, processes, systems, etc.
O3-94 [94] When sensitive or private information is sent over a network connection that is not limited to point-to-point connections, consideration should be given to encrypting that information before transmission.

R3-95 [95] The NE/NS shall provide a mechanism to deny the voice channel to a Customer Premises Equipment (CPE) if Black Box Fraud is suspected.20

R3-96 [96] The NE/NS shall provide mechanisms or procedures that can be used to periodically validate its correct operation (such as proper functioning of the security log, proper functioning of various trigger mechanisms, etc.).

R3-97 [97] The NE/NS shall provide mechanisms to monitor NE/NS resources and their availabilities (e.g., overflow indication, lost messages, buffer queues).

R3-98 [98] The NE/NS shall provide mechanisms to detect communication errors (relevant to the NE/NS) above a specifiable threshold.

O3-99 [99] The NE/NS should provide mechanisms to detect error conditions that might propagate throughout the NE/NS.

O3-100 [100] The NE/NS should provide mechanisms to periodically validate the correct operation of on-site hardware and firmware elements.

R3-101 [101] The NE/NS shall have the capability to protect data integrity by performing integrity checks and/or data update such as

... 1. Proper rule checking on data update

... 2. Adequate alert messages (e.g., "Do you really mean it?") in response to potentially damaging commands before executing them, so that involuntary human errors may be reduced

... 3. Proper handling of duplicate/multiple inputs

... 4. Checking return status

... 5. Checking intermediate results

... 6. Checking inputs for reasonable values

... 7. Proper serialization of update transactions.

20. For example, the CPE could be a PBX with "answer supervision" turned off.
R3-102 [102] The NE/NS shall provide a mechanism to generate a status report detailing the values of all parameters and flags that affect the secure operation of the system.

R3-103 [103] Administrator documentation shall contain recommendations for running, on a regular basis, integrity checking utilities for file systems or disks.

CR3-104[104] Where feasible, the file or disk integrity checking utilities shall be run automatically by vendor-supplied software.

3.7.1 Continuity of Service

The continuity of service feature deals with issues related to continuous accessibility and usability of NE/NS resources by an authorized user. It includes mechanisms and procedures that may reduce interference with time-critical operations, and allow the NE/NS to maintain its expected level of service in the face of any user action, deliberate or accidental, threatening this level of service.

O3-105 [105] The NE/NS should detect and report conditions that would degrade service (e.g., call processing) below a pre-specified minimum level.

CR3-106 [106] Depending on the application, i.e., if an NE/NS failure or discontinuity makes it vulnerable to security compromise, procedures or mechanisms shall be provided to allow "secure recovery" to reduce this threat.

R3-107 [107] The vendor shall have the capability to rebuild a base version and subsequent vendor modifications (e.g., patches) of the version, if that version and modifications are currently in use by a BCC. (This may not include BCC-specific data.)

R3-108 [108] The NE/NS shall provide adequate check points in a process flow of the software system so that, upon detection of a service deterioration, a recovery to an acceptable service level is facilitated. (Synchronization points, checkpoint restarts, etc., are typical examples for certain environments.)

3.8 Security Administration

Security Administration needs to conform to the layered architecture defined under TMN. There are many different security functions and parameters that must be administered to
implement the site-specific security policy. For example, the default values of various security parameters, as delivered by the vendor, have to be adjusted to meet the local requirements. The security parameters must be properly assigned and kept up to date so they can function satisfactorily. Security administration mechanisms, with appropriate interfaces, enable a human administrator to control the security of an NE/NS. This human administrator must be appropriately authorized to perform security administration and, in this document, is referred to as an "Appropriate Administrator." Typically, this function may be performed by a "System Administrator" or a separate "Security Administrator." Security Administration Functions must be reserved for a properly authorized Appropriate Administrator and must not be made accessible to unauthorized users in order to avoid the risk of abuse. In case remote security administration of several NEs is performed from a centralized OS facility over respective TL1 interfaces, it becomes necessary for the NE/NS to recognize those TL1 commands/messages and respond accordingly. TR-NWT-000835 provides a list of such commands/messages.

**R3-109** [109] The NE/NS shall support appropriate administrator functions as "separate" from other user functions. There shall be a mechanism such that the execution of these functions can be reserved only for an appropriate administrator (i.e., all other users shall be denied this permission).

**R3-110** [110] The security functions performed by an appropriate administrator shall be identified and documented.

**CR3-111** [111] If the option to enable or disable the administrator's account is an installation or run-time option of an NE/NS, the NE/NS shall not require that the account be enabled or activated during normal operation.

The NE/NS shall provide a mechanism for an appropriate administrator to

**R3-112** [112] Display all users currently logged on, where the word *user* is used in a broad sense as elsewhere in this document.

**R3-113** [113] Independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity.

**R3-114** [114] Independently and selectively monitor the activities of a specific terminal, port, or network address in real time.

**R3-115** [115] Authorize or revoke users.

**R3-116** [116] Lock out and restore a specific port or channel.

21. If the security log captures *all* activities over *all* channels, a capability of browsing the security log may satisfy this requirement.
R3-117 [117] Identify all resources accessible to any specific user (and to any specific channel, where applicable) along with the associated privileges required to access them.

R3-118 [118] Be denied creation of a user-ID that is already in use.

R3-119 [119] Disable a user-ID after a specifiable period of time during which the user-ID has not been used. Since unused accounts are a prime target for NE/NS intrusion, it is important that the list of active user-IDs is kept up to date.

R3-120 [120] Reinstate or delete disabled user-IDs, as a complementary mechanism or procedure.

R3-121 [121] Create or modify a password, and delete a user-ID along with all its attributes including the password.

R3-122 [122] *Not* be able to retrieve a password in clear text.

R3-123 [123] The following security parameters shall not be hard-coded (i.e., they shall be specifiable/assignable and adjustable by an appropriate administrator using operations-related messages):

1. Password Aging Interval, i.e., the length of time the password will remain valid after an being updated.

2. The interval (or equivalent) during which an expired password of a user shall be denied being selected again as a new password by the same user (to prevent "password flipping").

3. The events that may trigger alarms (e.g., failed login attempts), the levels of alarms (e.g., critical, major, minor), the type of notification (e.g., beep and/or message), and the routing of the alarm (e.g., specific port).

4. The duration of channel lock-out, which occurs when the threshold on the number of incorrect logins is exceeded.

5. A customized advisory warning banner that is displayed upon valid system entry regarding unauthorized use, and the possible consequences of violating the warning.

6. The duration of the time-out interval.

7. The privilege of a user to access a resource.

8. The privilege of a channel/port (for an NE/NS that has different input channels/ports for different operations functions) to access a resource.
9. Post-collection audit analysis tools for report generation (i.e., the NE/NS shall provide an appropriate administrator the capability to customize exception reports, summary reports, detailed reports, etc., on specific NE/NS data items, users, or communication facilities).

CR3-124 [124] Depending on the application, i.e., if the function of security administration is performed from a centralized facility (e.g., an OS) using TL1 language commands, the NEs/NSs shall comply with and appropriately respond to the Network Element and Network System Security Administration (NESSA) messages that are described in TR-NWT-000835.

CR3-125 [125] For an NE/NS that is required to provide a notification to users requiring them to change their passwords, the mechanism to accomplish this shall not be hard-coded (i.e., it shall be specifiable/assignable and adjustable by an appropriate administrator using operations-related messages). The following are examples of alternative ways to accomplish this:

- Adjusting the "early warning period" (i.e., how early shall the user be notified before the password expiration)
- Adjusting the "grace period" (i.e., the period over which an expired password is still accepted by the NE/NS)
- Adjusting the subsequent number of logins that will be allowed after password expiration.

R3-126 [126] An appropriate administrator shall have the capability to retrieve, copy, print, and upload a security log (typically to some OS or some other entity, for long-term storage).

R3-127 [127] An appropriate administrator shall not have the capability to modify or delete a security log.

R3-128 [128] An appropriate administrator shall have the capability to specify the condition (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload) that necessitates uploading the security log (typically to some OS or some other entity for long-term storage) to avoid an overwrite in the buffer.

O3-129 [129] An appropriate administrator should have the optional capability to record and maintain security log data in an encrypted form. If encryption is used, it should not employ the password encryption scheme because the
security log needs to be decrypted, while encrypted passwords must be protected from decryption.

R3-130 [130] An appropriate administrator shall have the capability to periodically validate the correct operation of the NE/NS (e.g., proper functioning of the security log, proper functioning of various trigger mechanisms).

R3-131 [131] An appropriate administrator shall have the capability to monitor NE/NS resources and their availabilities (e.g., overflow indication, lost messages, buffer queues).

R3-132 [132] An appropriate administrator shall have the capability to detect communication errors (relevant to the NE/NS) above an administrator-defined threshold.

O3-133 [133] The NE/NS should contain a real-time mechanism that is able to monitor the occurrence or accumulation of security-auditable events that may indicate an imminent security violation. (One such event, namely the malfunctioning of the security log, has already been defined as a requirement.) This mechanism should be able to immediately notify an appropriate administrator when administrator-defined thresholds are exceeded and, if the occurrence or accumulation of these security relevant events continues, the NE/NS shall take the least disruptive action to terminate the event.

R3-134 [134] When an NE/NS needs to be restarted, default user-IDs and passwords, previously modified by an administrator, shall not revert back to the vendor-delivered default user-IDs and passwords.
4. Development Life Cycle Requirements

NE/NS security features are not sufficient by themselves to provide a secure NE/NS. Security has to be considered throughout the entire development life cycle of the NE/NS as part of quality assurance and system reliability. All NE/NS features and mechanisms need to be properly conceived, designed, implemented, tested, installed, documented, and maintained. Otherwise, a false sense of security may result. This section describes the corresponding generic requirements. These requirements differ from those in the previous section in that they may not directly apply to Technical Analysis (i.e., Conformance Testing) of the security features of a vendor's end product. Instead, they provide baseline requirements related to quality assurance and reliability of security features during the development phase.

4.1 Security Policy

R4-1 [135] The NE/NS developer shall have a policy governing its internal development of software. The policy shall contain specific guidelines and requirements aimed at the security of its software systems and applicable throughout the software life cycle.

4.2 Requirement Analysis

CR4-2 [136] If the NE/NS is customized by the vendor for a specific application, a risk analysis shall be performed and documented to determine the degree of security required for that application. This shall include

… 1. Identification of typical data and software that are expected to be accessible via the NE/NS under the said application

… 2. Estimation of the impact if that data and software are compromised

… 3. Identification of the functions provided by the NE/NS under the said application, and the impact if they are made unavailable

… 4. Estimation of the potential risk if any deviations are made from conforming to the baseline requirements

… 5. Estimation of the potential risk to the expected NE/NS environment that may consist of networks, OSs, and other NEs/NSs

… 6. A characterization of the distribution of functions between the NE and the NS.

CR4-3 [137] For a customized NE/NS, application-specific security requirements shall be determined based on the risk analysis mentioned above. These
requirements shall be documented either in a stand-alone document or as part of a Requirements Specification.

R4-4 [138] The requirements shall consist of NE/NS security features described in this document, except where agreement is made with BCCs to differ.

CR4-5 [139] Depending on the application, i.e., if there are external or regulatory limitations imposed on data access, connectivity, etc., such limitations shall be taken into account. For example, if required by the BCC, the NE/NS shall provide partitioning for resource control to handle external user access so that unauthorized access requests can be denied.

4.3 System Design

R4-6 [140] The design shall not incorporate any mode of entry into the NE/NS that is not a documented feature of the NE/NS.

R4-7 [141] Functional security requirements shall be specified based on the high-level requirements defined during the Requirement Analysis.

R4-8 [142] Written documentation shall be produced describing the functional security requirements. This documentation shall be either a stand-alone document or part of a System Design Document.

R4-9 [143] The design shall accommodate separate user and appropriate administrator functions.

R4-10 [144] The security functions performed by an appropriate administrator shall be identified and documented.

CR4-11 [145] If it takes a privileged user (such as a superuser in a UNIX environment) to use or administer the NE/NS during the design phase, the privileged user-ID shall be distinct for the NE/NS.

CR4-12 [146] If the option to enable or disable a privileged user account is an installation or run-time option of an Operations Environment, the software shall not allow a nonprivileged user any means (e.g., typing "su" to become a superuser) to become privileged during a session established by the nonprivileged user.

R4-13 [147] Non-privileged users shall not be allowed access to the underlying Operating Environment of the NE/NS, unless the underlying Operating
Environment can maintain the resource access control policies and provide protection against loss of service.

### 4.4 Detailed System Design

**R4-14** [148] Detailed design shall incorporate security mechanisms that satisfy the functional security requirements defined during *System Design* and are based on the target Operating Environment, internal software design, transaction types, input screen layout, data and file structures, specific entry points, etc.

**R4-15** [149] Written documentation shall be produced describing the required security mechanisms. This documentation shall be either a stand-alone document or part of the product's *System Description*.

**R4-16** [150] Functional security requirements, as well as the potential for security flaws, shall be addressed during all detailed design reviews.

### 4.5 Implementation

**R4-17** [151] Security mechanisms defined during *Detailed System Design* shall be implemented.

**R4-18** [152] No method of access to the NE/NS (including access for software debugging) shall be provided other than that designed and documented during *System Design*.

**R4-19** [153] Passwords used during the design and implementation phase shall not be stored in clear text in unprotected databases or files.

**R4-20** [154] Occurrences of passwords in clear-text form within an executing program shall be overwritten immediately after use.

**R4-21** [155] All NE/NS software shall be treated as proprietary.

**R4-22** [156] All software source and object code modules shall have the proper proprietary markings.

**R4-23** [157] NE/NS vendors shall have documented policies and practices that provide guidelines to their developers on the legal protection of software intellectual property.
O4-24  [158]NE/NS vendor policies and practices that provide guidelines to their developers on the legal protection of software intellectual property should be available for review by BCCs.

CR4-25  [159]Depending on the application, i.e., if development is funded by a BCC for an application, the NE/NS vendor developers shall not copy or distribute the source or binary versions of the software outside of the development environment except through a BCC-authorized distribution mechanism.

4.6  Development Environment

R4-26  [160]NE/NS vendors shall have documented security policies and practices that address the secure usage and maintenance of their computer systems that are used in development of the NE/NS.

O4-27  [161]The NE/NS vendor security policies and practices that address the secure usage and maintenance of the vendor's computer systems used to develop the NE/NS should be available to the BCCs for review.

R4-28  [162]All systems used by the vendor in NE/NS development shall undergo periodic and documented internal security audits. A description of the audit procedures and the documentation of the occurrences of these audits (not necessarily the actual audit reports) shall be available to the BCCs for review. (This also reduces the risk of software viruses or bugs, such as trojan horses and trap doors, in software procured by a vendor from third parties.)

R4-29  [163]Passwords used by primary source code developers and other users of the development environment shall be kept private, not written down, and shall be subject to password complexity requirements described in this document.

R4-30  [164]Passwords required for remote access or for internal or external authentication mechanisms shall not be stored in clear-text in unprotected programs, files, or workstations.

R4-31  [165]Software used on any vendor development shall be legitimately obtained from an established commercial vendor or be approved by an appropriate authority (e.g., support groups of the involved systems, the development manager).
R4-32  [166]Public domain software and other types of software commonly distributed by, but not necessarily obtained from, public or private bulletin boards shall not be imported, used, or distributed by the vendor for use in the development environment unless

… 1. The software is available in source form

… 2. The source has been inspected and approved by an appropriate authority.

R4-33  [167]Software developed independently by employees shall be approved by an appropriate authority (e.g., support groups of involved systems, the development manager).

O4-34  [168]Developers should not use the development environment for business unrelated to the NE/NS development.

4.7  System Test

R4-35  [169]All security features shall be tested.

R4-36  [170]Tests shall include a search for flaws that would violate the generic security requirements described in this document.

R4-37  [171]Security features shall be a part of regression test suites.

R4-38  [172]All discovered flaws shall be corrected, removed, or neutralized and the NE/NS retested to demonstrate that they have been eliminated and that no new flaws have been introduced.

R4-39  [173]The developer or the testing organization shall document the test plan, test procedure, and test results.

O4-40  [174]The test plan, test procedure, and test results documentation should be available to the BCCs for review.
4.8 Packaging and Delivery

The initial installation of an NE/NS and each update to its system software ("generic") should be performed in a manner that does not compromise security.

R4-41 [175] Only authorized software and software modifications shall be added to the deliverable software baseline (or "generic").

R4-42 [176] All software changes shall be documented and reviewed to ascertain that security has not been compromised.

R4-43 [177] Tools or procedures shall exist for generation of a new version of the system software from backup media or source code.

R4-44 [178] Tools or procedures shall exist for protecting the backup media or source code from unauthorized modification.

R4-45 [179] Tools or procedures shall exist for verifying that a newly generated release contains the appropriate versions/levels of its component modules.

R4-46 [180] A combination of technical, physical, and procedural safeguards shall be used to protect the master copy or copies of all routines used to generate the system from unauthorized modification or destruction.

R4-47 [181] A master database shall be maintained of all delivered instances of the NE/NS software that includes the software release number.

CR4-48 [182] A master database shall be maintained of all delivered instances of the NE/NS software that includes the specific release of Operating Environment or associated software with which the NE/NS software is being run, if it is necessary for the proper packaging or distribution of the NE/NS.

R4-49 [183] All NE/NS generics shall be provided with secure installation defaults.

R4-50 [184] All default user-IDs that are delivered with the NE/NS generic shall be delivered with their corresponding passwords (typically agreed upon by the BCC and the vendor), which shall be modifiable by an appropriate administrator in the BCC any time during the vendor and BCC installation processes.

R4-51 [185] Though requiring a site security acceptance test is not a vendor responsibility, procedures for such testing shall be provided to determine
whether the NE/NS software updates delivered to a BCC are exactly as specified by the master copies.

**R4-52** [186] Procedures (e.g., use of modification dates, permissions, checksums) shall exist that make it possible to verify, at any time, that the currently installed software has remained consistent with the delivered software, i.e., no unauthorized modifications have been made.

**R4-53** [187] Vendor documentation shall accompany the delivered software.

### 4.9 Documentation

The security features of an NE/NS can be ineffective without adequate documentation of these features and the methods and procedures to administer them.

**R4-54** [188] Instructions and documentation on security considerations shall be provided separately for Users, Appropriate Administrators, and Operators.

**R4-55** [189] The documentation on security considerations shall either be provided in stand-alone documents or embedded in other existing documents, such as the *System Administration Guide, System Operations Guide*, or *User Guide* for the NE/NS.

**CR4-56** [190] Depending on the application, documentation can be in the form of hard copy or electronic files retrievable by the BCCs. If documentation is available as electronic files, unauthorized access to the information shall be denied.

**CR4-57** [191] If documentation is available online, the documentation shall have the appropriate proprietary markings.

**R4-58** [192] End-user documentation shall not contain any information that could jeopardize the security of the NE/NS if made public. For example, no actual passwords shall be listed in the documentation.

**R4-59** [193] The *User Guide* shall describe the protection mechanisms that are non-transparent to the user, explain their purpose, and provide guidelines on their use.

**R4-60** [194] The *System Administration Guide* shall contain

… 1. Cautions about functions and privileges that need to be controlled when running a secure facility
... 2. Documentation on the use of all security audit tools, including
... • Procedures for examining and maintaining the audit files
... • Detailed audit record structures for each type of audit event
... • Procedures for periodic backup of security logs
... 3. Administrator functions related to security, including adding or
deleting a user, changing the security characteristics of a user, etc.
... 4. Recommendations on setting the minimum access permissions on all
files, directories, and databases
... 5. Guidelines on the consistent and effective use of the protection
features of the NE/NS, and how they interact
... 6. Guidelines on security self-assessment techniques that cover areas
such as security reports for line management, password requirements,
and dial-access restrictions.

O4-61 [195] The System Administration Guide should contain documentation on
the use of procedures for checking the amount of free space available for
the log files.

R4-62 [196] The System Operations Guide shall contain
... 1. Procedures necessary to initially start the NE/NS in a secure manner
... 2. Procedures to resume secure NE/NS operations after any lapse in NE/
NS operation.

R4-63 [197] Developers shall not copy or distribute internal documentation
outside of the development environment except through an authorized
distribution mechanism.

4.10 Support

R4-64 [198] The vendor shall designate a team as the primary contact and provide
a backup contact for security issues regarding the NE/NS.

R4-65 [199] A method for notifying customers of new security problems shall be
documented and followed.

R4-66 [200] All security problems that pose a security threat, including those
identified by the BCCs, shall be characterized and treated as having high
severity until resolved or downgraded with the consent of the relevant BCCs.

CR4-67 [201] If security flaws are observed by the vendor for a supported release of the NE/NS software, the flaws shall be made available to the BCC on a Proprietary/Restricted basis.

CR4-68 [202] If feasible, fixes to security flaws in each supported release of the NE/NS software shall be available without having to upgrade to the next release of the NE/NS.

O4-69 [203] Security enhancements and corrections should be independent of a release, i.e., the flexibility should exist to install security changes independently of other NE/NS modifications.

R4-70 [204] All BCC system login information, including user-ID, password, and telephone numbers of dial-in ports, shall be treated as Proprietary/Restricted.

R4-71 [205] Vendor personnel shall not access any BCC NE/NS without prior authorization from the BCC.

R4-72 [206] Vendor personnel shall follow all BCC rules for NE/NS access and not bypass BCC security procedures.

R4-73 [207] The development, testing, or installation of new features, patches, or "quick fixes" shall not take place on a BCC's live NE/NS without an "appropriate level of authorization" from the BCC's management.

R4-74 [208] All new features, patches, or "quick fixes" shall be tested first on a development system or approved by an appropriate "system test" organization.

R4-75 [209] Sanity tests or acceptance tests, which modify "live" data, shall not be done.

CR4-76 [210] If modifications/enhancements are made to the NE/NS that may influence the sensitivity of items, such as data typically resident in the NE/NS and typical interfaces and functions of the NE/NS, a determination shall be made of the potential impact of such modifications/enhancements on the security of the NE/NS.
R4-77 [211] Any changes to the functionality or installation defaults of security mechanisms in a new release shall be documented and the documentation made available to the BCC before the shipment of that release.

R4-78 [212] All maintenance and new feature releases shall be subject to the entire set of Development Life Cycle security requirements.

R4-79 [213] New releases shall not be made generally available until after all documentation and system testing has been completed.

R4-80 [214] Documentation shall be provided describing the secure setup and installation of a new system release. This documentation shall include a discussion of all BCC-visible security-related procedures, software, and data files.
5. Telecommunications Management Network (TMN)

The TMN was (and is) being developed in order to support interoperability among OSs, NEs, workstations, and external entities for the purpose of network management, i.e., to plan, provision, install, maintain, operate and administer telecommunications networks and services. Interoperability is achieved through standard interfaces. The communication protocols for these interfaces are defined in ITU-T Recommendations Q.811 and Q.812. These recommendations support both the “classical” OSI stack, as well as TCP/IP transport.

Network management interoperability requires that two communicating systems have a common view of the resource that is being managed (e.g., a SONET ADM) and a common way of exchanging management information about that resource. Such common views are provided by standard information models. In order to facilitate the task of developing such information models, the TMN divides network management functions into five layers and five functional areas (ITU-T Rec. M.3400).

The TMN classifies network management functions into a layered architecture consisting of five layers. In a descending order of hierarchy, they are: (i) the Business Management Layer (BML), (ii) the Service Management Layer (SML), (iii) the Network Management Layer (NML), (iv) the Element Management Layer (EML), and (v) the Network Element Layer. In addition, there are five Management Functional Areas:

1. Configuration Management - It is responsible for planning and installation of NEs/NSs, their interconnection into a network, and the establishment of customer services that use the network.

2. Performance Management - It evaluates and reports upon the behavior of telecommunications equipment and the effectiveness of the network and NEs/NSs for the support of services.

3. Fault Management - It enables the detection, isolation, and correction of abnormal operation of the telecommunications network and its environment.

4. Accounting Management - It enables the use of the network services to be measured and the cost of such use to be determined. It provides facilities to collect accounting records and to set billing parameters for the usage of services and for periodic charges for access to the network. It also includes enterprise control functionality to exercise diligence over the proper flow of funds within the enterprise and between the enterprise and its owners and creditors.

5. Security Management - It provides for prevention and detection of improper use of network resources and services, for the containment of and recovery from theft of services or other breaches of security, and for security administration.

The TMN may be used to manage NEs/NSs on an individual or collective basis where the collection consists of NEs/NSs having a set of common characteristics or capabilities. Examples of NE/NS collections are
5. Equipment type of NEs such as a collection of SONET ADMs
2. Topology such as interconnected Asynchronous Transfer Mode (ATM) switches
3. NEs/NSs that meet a particular service or customer need, such as a collection of NEs to provide video services or a customer's private network
4. NEs/NSs associated with an administrative domain, such as all the NEs/NSs served by a single maintenance service center.

5.1 TMN Security

Security management consists of functions such as:

1. **Prevention** - physical security, legal review, personnel risk analysis, logical controls
2. **Detection** - customer and user usage pattern analysis, investigation of changes of revenue pattern, investigation of theft of resources and service, inspection of systems such as: (i) heating, ventilation and air conditioning (HVAC), (ii) fire protection, (iii) flood protection, and (iv) security alarm
3. **Containment and Recovery** - legal action, apprehension, disaster recovery, network intrusion recovery
4. **Security Administration** - described in some detail in the next section.

5.2 TMN Layers for Security Administration

An illustration is now provided as to how the overall functionality of "Security Administration" can be delineated according to the five layers of TMN.

1. **BML** - security policy, disaster recovery planning, assessment of data integrity
2. **SML** - administration of certification, administration of security protocols, customer audit trail management, customer security alarm management
3. **NML** - administration of security parameters at the overall network level.
4. **EML** - administration of security parameters of a group of similar NEs/NSs, such as several SONET ADMs
5. **NEL** - updating NE/NS parameters from the craft console at the NE/NS.

5.3 Securing the TMN

Several national and international standards (will) provide useful guidance to securing a TMN:
In order to secure TMN transactions an NE/NS should conform to the following objectives:

**O5-1** [215] An NE/NS should include STASE-ROSE in the application layer of its OSI protocol stack

**O5-2** [216] An NE/NS should include a Directory User Agent (DUA) in order to access the TMN directory for the purpose of retrieving public key certificates (as well as other network management information)

**O5-3** [217] An NE/NS should support all the default algorithms of STASE-ROSE

### 5.4 Managing TMN security

Bellcore GR-1253-CORE provides detailed information models for managing security information. Whenever applicable, the models in GR-1253 are based on existing
international standards. In order to facilitate the management of security-related information (passwords, keys, access control privileges) the TMN should include a secure directory, as specified in ANSI T1.252, to manage security information. In order to allow remote management of security information, an NE/NS should support the relevant information models in GR-1253 in the Agent role.


**NOTE:**

All Bellcore documents are subject to change, and their citation in this document reflects the most current information available at the time of this printing. Readers are advised to check current status and availability of all documents.

To obtain Bellcore documents, contact:

Bellcore Customer Service
8 Corporate Place, Room 3A-184
Piscataway, New Jersey 08854-4156
1-800-521-CORE (2673) (US & Canada)
(732) 699-5800 (all others)
(732) 336-2559 (FAX)

BCC personnel should contact their company document coordinator, and Bellcore personnel should call (732) 699–5802 to obtain documents.
Glossary

ADM — Add-Drop Multiplexer

Appropriate Administrator — A highly privileged person (e.g., system administrator, security administrator) who is authorized to perform security-related administrative tasks.

ANI — Automatic Number Identification

BCC — Bellcore Client Company, meaning any divested Bell Operating Company, or its successor, or any regional affiliate thereof

CCITT — International Telegraph and Telephone Consultative Committee

CCS — Common Channel Signaling

CRUD — Operations functions related to creating, retrieving, updating, and deleting NE/NS resources

Customer — A person or an organization that is a subscriber to a service offered by a BCC

CW — Call Waiting, a service feature associated with a record in the subscriber line view of a circuit switch.

EAI — Emergency Action Interface, a port that allows access into an NE/NS (typically without system access control) to restore the NE/NS in an emergency.

EMS — Element Management System, which performs several operations related functions for an NE/NS (especially for broadband applications) in accordance with the TMN architecture

HVAC — Heating, Ventilation, and Air Conditioning

ITS — Integrated Testing System

MAS — Memory Administration System

MC — Major Class, a Service/Resource parameter associated with a record in the subscriber line view of a circuit switch

MML — Man Machine Language

NE/NS — Network Element or Network System - typically NE implies circuit switches, packet switches, and various transmission elements, whereas NS encompasses adjuncts, intelligent peripherals, EMS, etc.

NESSA — Network Element and Network System Security Administration - NESSA messages are used to perform CRUD functions on security-related parameters in the NE/NS (TR-NWT-000835 describes these messages and the corresponding NE/NS responses)

NIST — National Institute of Standards
NMA

and Technology

**NMA** — Network Monitoring and Analysis, an Operations Systems for Network Surveillance and Maintenance

**NMS** — Network Management System, an Operations System for management of the entire network (including security management) in conformance with the layered architecture of the TMN

**NSA** — National Security Agency

**NSSOG** — National Security Telecommunications Advisory Committee

**OA&M** — Operations, Administration, and Maintenance, operations-related functions, typically performed from appropriate OSs

**OS** — Operations System, a software application that supports operations such as provisioning, maintenance, testing, billing, etc., related to NEs/NSs

**PBX** — Private Branch Exchange, a switch that is typically deployed as a Customer Premises Equipment (CPE)

**PSN** — Public Switched Network

**Privileged User** — A user that is allowed additional data, transactions, or service access (i.e., beyond the access rights of normal users), e.g., a superuser in a UNIX environment

**R**

**Resource** — Any nameable entity under the control of the NE/NS that can be accessed by a user (e.g., processes, programs, databases, files, memory, disks)

**RFP** — Request for Proposal, announced by a prospective procurer to express the intent of procurement, so that interested suppliers may respond

**S**

**SCP** — Service Control Point

**SONET** — Synchronous Optical Network, provides a transport technology (i.e., transmission) over optical networks

**SS7** — Signaling System 7 (Protocol for CCS)

**T**

**Technical Analysis** — Conformance testing of the features of a vendor product against feature requirements for that product as described in an appropriate Technical Reference document

**TL1** — Transaction Language 1, a language developed by Bellcore, primarily for an OS-to-NE/NS interface, based on the syntax of CCITT/MML

**TMN** — Telecommunications Management Network

**U**

**User** — A person, process, or system (e.g., an OS) accessing or attempting to access an NE/NS for the purpose of
User-ID

performing operations-related tasks

User-ID — A non-confidential “name” by which a valid user of an NE/NS is unambiguously recognized by the NE/NS
User-ID