Pakistan Telecom Authority

Telecommunication Security Guidelines

Contents

Intoduction:

1. The global telecommunication market is rapidly transforming. Telecom networks are undergoing astounding changes with deployment of all-IP Next Generation Networks. Together with these developments and evolvement of a global information space, new types of security threats have emerged. Criminals are using Telephone, Internet and Mobile networks for committing various kind of crimes categorized under electronic crimes.

Security is a pervasive aspect of information & communication systems; performance and cost. Keeping in view the rapid telecommunication development experienced during recent years, it is imperative that our distributed information and communication systems and networks should be made attack resistant, by a combination of technical, organizational and legal measures.

In this regard Pakistan Telecommunication Authority established an expert group on ICT security in coordination with ICT Industry to discuss and scrutinize potential security threats faced by information and communication networks of the country. The group was divided into three sub-groups (Telecommunication, Government of Pakistan and End-user) for exploring potential security areas and drafting guidelines to address them.

The "Telecom Security Guidelines" provide a compact overview of the most important organizational, infrastructural and technical telecom security safeguards. These guidelines are intended to satisfy this need, providing a compact and easily understandable overview of the most relevant security safeguards.

ICT Security in Focus:

2. Security is a basic need of human beings, and hence of our society. Especially in the era of globalization, rising mobility and growing dependence on information and communication technology by the industrial nations, this need for security is becoming ever more pronounced.

Increased vulnerability and the threat of massive financial damage as a result of ICT problems are augmenting the pressure to take action to prevent damage and minimize the residual risk through active ICT security management. Responsibility is not confined to the ICT departments concerned. On the contrary, security is a managerial issue. And, moreover, the legislator has recognized this. Various laws and regulations now make directors personally responsible should they fail to take the required action.

It is widely believed that ICT security safeguards demand high investment and that their implementation requires highly skilled personnel. However, this is not the case. The main ingredients of success are common sense, well thought out organizational procedures and guidelines, well informed staff who independently and expertly observe security requirements in a disciplined manner. The creation and implementation of an effective ICT security concept therefore need not necessarily be expensive.

Another widely held misconception concerns the actual protection requirement. Often one hears remarks like:

"Nothing ever happened to us so far" A brave statement to make. It is perfectly possible that there have been security incidents before but that went unnoticed.

"Why would anyone want to attack us, our data is not confidential" In most cases, such a view is too outward. When taking a closer look at damage scenarios, it soon becomes clear: some of the data that is processed can be misused in a variety of ways if in the wrong hands.

"Our network is secure" Often the capabilities of potential hackers are underestimated. Moreover, even an experienced network or security specialist should not know everything and can make mistakes. External audit and reviews always uncover serious vulnerabilities and are a good protection against **"operational blindness".**

"Our staff can be trusted." A variety of statistics show a different picture: the majority of security breaches are caused by insiders. These security breaches do not always involve malicious intent. Serious damage can also be occasioned by mistake or curiosity coupled with a lack of awareness.

Everyone has to recognize that security is not a static state but an ongoing process. Therefore one should constantly ask himself the following questions:

- If confidential information from your organization fall into the hands of third parties how could it be improperly used?

- What would be the consequences if important information were modified, for example, during data transmission or on your server? The cause does not need to be malicious intent on the part of unknown third parties but could also be a technical failure.

- What would happen if vital servers or other ICT components in your organization suddenly failed and could no longer be used for an extended period (days, weeks etc.)? Would everyone be able to continue their work? How extensive could the damage be?

3. Important Concepts Relating to ICT Security :

There are three core values of ICT security: confidentiality, availability and integrity.

Confidentiality: information that is confidential must be protected against unauthorized disclosure.

Availability: services, system functions, data and information must be available to users as required.

Integrity: data and information must be complete and unaltered.

Some other terms frequently used are:

Authentication: When a person logs in on a system, the system runs a check in an authentication process to verify the identity of the person. The term is also used when the identity of ICT components or applications is tested.

Authorization: Authorization is the process of checking whether a person, an ICT component or an application is authorized to perform a specific action.

Data protection: Data protection refers to the protection of personal data against misuse by third parties.

Data security: Data security refers to the protection of data in respect of requirements on its confidentiality, availability and integrity. An alternative term for this is “ICT security“.

Data backup: Data backup involves making copies of existing data to prevent its loss.

Penetration testing: Penetration testing is a directed, normally simulated attack on an IT system. It is used as a test of the effectiveness of existing security safeguards.

Risk assessment or analysis: A risk analysis provides information on the probability of the occurrence of a damaging event and what negative consequences the damage would have.

Security policy: In a security policy the security objectives and general security safeguards are formulated in the sense of the official regulations of a company.

4. Security Functions :

Security objectives can be achieved and maintained to a given degree of predictability against threat agents and processes by apply a number of different abstract security functions. A complete chain or continuum of security functions begins with deterrence and ends with recovery.

Deter Deterrence can be achieved using a number of different means depending on whom or what the threat agents are. A simple banner warning on a WebPages can be used for some attackers while for advanced attackers, long encryption keys can be used to deter exhaustive key searches.

Protect the two basic means to protect a system are either to allow or deny access to individuals or processes as they attempt to enter or use a system.

Control the two basic means to protect a system are either to allow or deny access to individuals or processes as they attempt to enter or use a system.

Monitor once the protection functions are covered, the next abstract security function is to detect individuals or process that have violated the protection or to monitor those individuals or process which have been granted access to the system and have the possibility to violate security procedures.

Respond once detection of a security event has occurred there must be functions in the systems to respond to such the event in an appropriate and timely manner.

Recover if none of the security functions above have succeeded in stopping the threat agent or process there should be function in place to recover from a security violation.

5. Security Framework Requirement:

The requirement for a generic network security framework has been originated from different sources:

- Customers/subscribers need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes (including terrorist actions).
- Public authorities demand security by directives and legislation, in order to ensure availability of services, fair competition and privacy protection.
- Network operators and service providers themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public.

Security requirements for telecommunication networks and services should preferably be based upon internationally agreed security standards, as it increases interoperability as well as avoids duplication of efforts and reinventing the wheel. The provisioning and usage of security services and mechanisms can be quite expensive relatively to the value of the transactions being protected. There is a balance to consider between the cost of security measures and the potential financial effects of security breaches.
It is therefore important to have the ability to customize the security provided in relation to the services being protected. The security services and mechanisms that are used should be provided in a way that allows such customization. Due to the large number of possible combinations of security features, it is desirable to have security profiles that cover a broad range of telecommunication network services.

6. General Telecommunication Security Guidelines

Single Point of Failure

Network Operators and Service Providers should, where appropriate, design networks to minimize the impact of a single point of failure (SPOF).

Network Monitoring

Network Operators and Service Providers should monitor the network to enable quick response to network issues.

Ingress Filtering

Network Operators and Service Providers should, where feasible, implement RFC 3704 ingress filtering.

Routing Resiliency

Network Operators and Service Providers should use virtual interfaces (i.e. a router loopback address) for routing protocols and network management to maintain connectivity to the network element in the presence of physical interface outages.

Route Aggregation

Network Operators and Service Providers should aggregate routes where appropriate (e.g., singly-homed downstream networks) in order to minimize the size of the global routing table.

CIDR Use

Network Operators and Service Providers should enable CIDR (Classless Inter-Domain Routing) by implementing classless route prefixes on routing elements.

BGP Authentication

Network Operators and Service Providers should authenticate BGP sessions (e.g., using TCP MD5) with their own customers and other providers.

Route Exchange Limits

Network Operators and Service Providers should set and periodically review situation-specific limits on numbers of routes imported from peers and customers in order to lessen the impact of mis-configurations.

Route Flapping

Network Operators and Service Providers should manage the volatility of route advertisements in order to maintain stable IP service and transport. Procedures and systems to manage and control route flapping at the network edge should be implemented.

Route Policy

Network Operators and Service Providers should have a route policy that is available, as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting.

Route Database

Network Operators and Service Providers should operate a route database. That database should provide the routing advertisement source from the Network Operator's perspective. The database should be accessible by peers, customers and other users. The access can be via a web interface similar to the looking glass server's or just telnet access. The database is informational only and can not be used

to effect or impact the actual routing table. The need to provide security and isolation to such a database is high.

Route Registry Database

Network Operators and Service Providers should operate a route registry database of all the routes advertised by their network with the source of that advertisement. This database might be used as the source for interface configurations as well as troubleshooting problems. If an entity decides to operate a central route registry for a region or globally, the individual Service Provider database can communicate with that central repository forming a robust and efficient hierarchical system.

End-to-End Path Monitoring

Network Operators and Service Providers should consider measuring end-to-end path performance and path validity for both active and alternate routes.

Route Controls

Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions.

Software & Hardware Vulnerability Tracking

Operators and Service Providers should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. These reports and recommendations are typically provided by equipment suppliers.

SPAM Control

Network Operators and Service Providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.

Role-based Mailbox

Network Operators and Service Providers should, for easy communication with subscribers and other operators and providers, use of specific role-based accounts (e.g., abuse@provider.net, ip-request@provider.net) versus general accounts (e.g., noc@provider.net) which will help improve organizational response time and also reduce the impact of Spam.

Attack Trace Back

Network Operators, Service Providers and Equipment Suppliers should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a

destination of network to block service or consume resources to overflow state that might cause system crashes).

Telecom Equipment Manufacturing

Equipment Suppliers should establish and use metrics to identify key areas and measure progress in improving quality, reliability, and security during product development and field life cycle.

Congestion Control

Network Operators and Service Providers implementing protocols for the transport of VoIP data on IP networks should implement congestion control mechanisms such as those described by RFC 2309, RFC 2914, and RFC 3155.

TCP Configuration

Network Operators should configure their TCP algorithm parameters according to RFC 3481 in order to optimize the performance of TCP/IP data transport over 2.5G and 3G wireless networks.

VoIP Coding Standards

Service Providers should consider using a minimum interoperable subset for VoIP coding standards (for example, TI 811 mandates the use of G.711) in a VoIP-to-PSTN gateway configuration in order to achieve interoperability and support all types of voice band communication (e.g., DTMF tones, facsimile, TTY/TDD).

SS7 Network Management Control

Wireless Service Providers who have deployed GSM Mobility Application Part (MAP) signaling networks should consider implementing and using the network management controls of SS7 within their networks.

Traffic Policies

Service Providers should consider appropriate means for providing their customers with information about their traffic policies so that users should be informed when planning and utilizing their applications.

Collaborative Operation Standards

Service Providers, Network Operators and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless).

Network Performance

Service Providers should make available meaningful information about expected performance with respect to upstream and downstream throughput and any limitations of the service; best effort services "up to" or unspecified bit rate services should be specified as such in a clearly identifiable manner. Specified rate services

(such as those covered by QoS or similar systems) should be handled by an SLA between the parties.

Residential Internet Access

For the deployment of Residential Internet Access Service, Broadband Network Operators should design in the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance, security, or usage policy. For the deployment of Residential Internet Access Service, in a shared media environment, Service Providers should design Broadband systems that provide appropriate privacy and access restriction to the data packet information (eg. DOCSIS, PON).For the deployment of Residential Internet Access Service, a Broadband Network Operator should incorporate multilevel security schemes for network data integrity, as applicable, in the network design to prevent user traffic from interfering with network operations, administration, and management use.

Remote Access / Disaster Recovery Strategy

Network Operators and Service Providers should consider creating a corporate policy statement that defines a remote system access strategy, which should include a special process for disaster recovery.

Security Management Functions

Network Operators, Service Providers and Equipment Suppliers should consider establishment of a senior management function for a chief security officer (CSO) or functional equivalent to direct and manage both physical and logical security.

Strong Encryption Algorithms and Keys

Network Operators, Service Providers, and Equipment Suppliers should use industry-accepted algorithms and key lengths for all uses of encryption, such as AES or AES finalists.

Control Plane Reliability

Network Operators and Service Providers should minimize single points of failure (SPOF) in the control plane architecture (e.g., Directory Resolution and Authentications services). Critical applications should not be combined on a single host platform. All security and reliability aspects afforded to the User plane (bearer) network should also be applied to the Control plane network architecture.

Protection of Externally Accessible Network Applications

Network Operators and Service Providers should protect servers supporting externally accessible network applications by preventing the applications from running with high-level privileges and securing interfaces between externally accessible servers and back-office systems through restricted services and mutual authentication.

Network Architecture Isolation/Partitioning

Network Operators and Service Providers should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested the user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks be separated and partitioned from one another.

OAM&P Product Security Features

Equipment Suppliers should implement current industry baseline requirements for Operations, Administration, Management, and Provisioning (OAM&P) security in products, network elements, and management systems.

Secure Communications for OAM&P Traffic

To prevent unauthorized users from accessing Operations, Administration, Management, and Provisioning (OAM&P) systems, Network Operators and Service Providers should use strong authentication for all users. To protect against tampering, spoofing, eavesdropping, and session hijacking, Service Providers and Network Operators should use a trusted path for all important OAM&P communications between network elements, management systems, and OAM&P staff.

OAM&P Privilege Levels

For OAM&P systems, Network Operators and Service Providers should use element and system features that provide "least-privilege" for each OAM&P user to accomplish required tasks using role-based access controls where possible.

Segmenting Management Domains

For OAM&P activities and operations centers, Network Operators and Service Providers should segment administrative domains with devices such as firewalls that have restrictive rules for traffic in both directions and that require authentication for traversal. In particular, segment OAM&P networks from the Network Operator's or Service Provider's intranet and the Internet. Treat each domain as hostile to all other domains. Follow industry recommended firewall policies for protecting critical internal assets.

OAM&P Protocols

Network Operators, Service Providers and Equipment Suppliers should use Operations, Administration, Management and, Provisioning (OAM&P) protocols and their security features according to industry recommendations. Examples of protocols include SNMP, SOAP, XML, and CORBA.

Hardening OAM&P User Access Control

Network Operators, Service Providers and Equipment Suppliers should, for OAM&P applications and interfaces, harden the access control capabilities of each network element or system before deployment to the extent possible (typical steps are to remove default accounts, change default passwords, turn on checks for password complexity, turn on password aging, turn on limits on failed password attempts, turn on session inactivity timers, etc.) A preferred approach is to connect each element or system's access control mechanisms to a robust AAA server (e.g., a RADIUS or TACAS server) with properly hardened access control configuration settings.

Expedited Security Patching

Network Operators, Service Providers and Equipment Suppliers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available. Such processes should include determination of when expedited patching is appropriate and identifying the organizational authority to proceed with expedited patching. This should include expedited lab testing of the patches and their effect on network and component devices.

Limited Console Access

Network Operators, Service Providers and Equipment Suppliers should not permit users to log on locally to the Operation Support Systems or network elements. System administrator console logon should require as strong authentication as practical.

SNMP Vulnerability Mitigation

Network Operators, Service Providers and Equipment Suppliers should apply SNMP vulnerability patches to all systems on infrastructure networks because SNMP vulnerabilities can create significant risk.

Source, Object, and Binary Code Integrity

Network Operators and Service Providers should use software change management systems that control, monitor, and record access to master source of software. Ensure network equipment and network management code consistency through checks such as digital signatures, secure hash algorithms, and periodic audits.

Distribution of Encryption Keys

When Network Operators, Service Providers and Equipment Suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that: a) Ensures the authenticity of the recipient, b) Does not depend upon secure transmission facilities, and c) Cannot be emulated by a non-trusted source.

Network Access to Critical Information

Network Operators and Service Providers and Equipment Suppliers should carefully control and monitor the networked availability of sensitive security information for critical infrastructure by

- Periodic review public and internal website, file storage sites HTTP and FTP sites contents for strategic network information including but not limited to critical site locations, access codes.
- Documenting sanitizing processes and procedures required before uploading onto public internet or FTP site.
- Ensuring that all information pertaining to critical infrastructure is restricted to need-to-know and that all transmission of that information is encrypted.
- Screening, limiting and tracking remote access to internal information resources about critical infrastructure.

Software Development

Network Operators, Service Providers and Equipment Suppliers should adopt internationally accepted standard methodologies, such as ISO 15408 (Common Criteria) or ISO 17799, to develop documented Information Security Programs that include application security development lifecycles that include reviews of specification and requirements designs, code reviews, threat modeling, risk assessments, and training of developers and engineers.

System Inventory Maintenance

Network Operators and Service Providers should maintain a complete inventory of elements to ensure that patches/fixes can be properly applied across the organization. This inventory should be updated each time a patch/fix is identified and action is taken.

Security Evaluation Process

For Network Operators and Service Providers, a formal process during system or service development should exist in which a review of security controls and techniques is performed by a group independent of the development group, prior to deployment. This review should be based on an organization's policies, standards, and guidelines, as well as best practices. In instances where exceptions are noted, mitigation techniques should be designed and deployed and exceptions should be properly tracked. Patch/Fix Verification: Network Operators and Service Providers should perform a verification process to ensure that patches/fixes are actually applied as directed throughout the organization. Exceptions should be reviewed and the proper patches/fixes actually applied.

Mitigate Control Plane Protocol Vulnerabilities

Network Operators and Service Providers should implement architectural designs to mitigate the fundamental vulnerabilities of many control plane protocols (eBGP, DHCP, SS7, DNS, SIP, etc): 1) Know and validate who you are accepting information from, either by link layer controls or higher layer authentication, if the protocol lacks authentication. 2) Filter to only accept/propagate information that is reasonable/ expected from that network element/peer.

BGP (Border Gateway Protocol) Validation

Network Operators and Service Providers should validate routing information to protect against global routing table disruptions. Avoid BGP peer spoofing or session hijacking.

Prevent BGP (Border Gateway Protocol) Poisoning

Network Operators and Service Providers should use existing BGP filters to avoid propagating incorrect data. Options include:

- Avoid route flapping DoS by implementing RIPE-229 to minimize the dampening risk to critical resources,
- Stop malicious routing table growth due to de-aggregation by implementing Max-Prefix Limit on peering connections,
- Employ ISP filters to permit customers to only advertise IP address blocks assigned to them,
- Avoid disruption to networks that use documented special use addresses by ingress and egress filtering for "Martian" routes,
- Avoid DoS caused by un-authorized route injection (particularly from compromised customers) by egress filtering (to peers) and ingress filtering (from customers) prefixes set to other ISPs,
- Stop DoS from un-allocated route injection (via BGP table expansion or latent backscatter) by filtering "bogons" (packets with unauthorized routes), not running default route or creating sink holes to advertise "bogons", and
- Employ "Murphy filter" (guarded trust and mutual suspicion) to reinforce filtering your peer should have done.

Protect Interior Routing Tables

Network Operators should protect their interior routing tables with techniques such as 1) Not allowing outsider access to internal routing protocol and filter routes imported into the interior tables 2) Implementing MD5 between IGP neighbors.

Protect DNS (Domain Name System) Servers against Compromise

Network Operators and Service Providers should protect against DNS server compromise by implementing protection such as physical security, removing all unnecessary platform services, monitoring industry alert channels for vulnerability exposures, scanning DNS platforms for known vulnerabilities and security breaches, implementing intrusion detection on DNS home segments, not running the name server as root user/minimizing privileges where possible, and blocking the file system from being compromised by protecting the named directory.

Protect Against DNS (Domain Name System) Denial of Service

Network Operators and Service Providers should provide DNS DoS protection by implementing protection techniques such as:

- Increase DNS resiliency through redundancy and robust network connections
- Have separate name servers for internal and external traffic as well as critical infrastructure, such as OAM&P and signaling/control networks
- Where feasible, separate proxy servers from authoritative name servers
- Protect DNS information by protecting master name servers with appropriately configured firewall/filtering rules, implement secondary masters for all name resolution, and using Bind ACLs to filter zone transfer requests.

MPLS (Multi-Protocol Label Switching) Configuration Security

Network Operators and Service Providers should protect the MPLS router configuration by

- Securing machines that control login, monitoring, authentication and logging to/from routing and monitoring devices
- Monitoring the integrity of customer specific router configuration provisioning
- Implementing (e)BGP filtering to protect against labeled-path poisoning from customers/peers.

Network Access Control for SS7

Network Operators should ensure that SS7 signaling interface points that connect to the IP Private and Corporate networks interfaces are well hardened, protected with packet filtering firewalls; and enforce strong authentication. Similar safeguards should be implemented for e-commerce applications to the SS7 network. Network Operators should implement rigorous screening on both internal and

interconnecting signaling links and should investigate new, and more thorough screening capabilities. Operators of products built on general purpose computing products should proactively monitor all security issues associated with those products and promptly apply security fixes, as necessary. Operators should be particularly vigilant with respect to signaling traffic delivered or carried over Internet Protocol networks. Network Operators that do employ the Public Internet for signaling, transport, or maintenance communications and any maintenance access to Network Elements should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).

SS7 Authentication

Network Operators should mitigate limited SS7 authentication by enabling logging for SS7 element security related alarms on SCPs and STPs, such as: unauthorized dial up access, unauthorized logins, logging of changes and administrative access logging. Network operators should implement rigorous screening on both internal and interconnecting signaling links and should investigate new, and more thorough screening capabilities. Operators of products built on general purpose computing products should proactively monitor all security issues associated with those products and promptly apply security fixes, as necessary. Operators should establish login and access controls that establish accountability for changes to node translations and configuration. Operators should be particularly vigilant with respect to signaling traffic delivered or carried over Internet Protocol networks. Network operators that do employ the Public Internet for signaling, transport or maintenance communications and any maintenance access to Network Elements shall employ authentication, authorization, accountability, integrity and confidentiality mechanisms (e.g. digital signature and encrypted VPN tunneling). Operators making use of dial-up connections for maintenance access to Network Elements should employ dial-back modems with screening lists. One-time tokens and encrypted payload VPNs should be the minimum.

SS7 DoS Protection

Network Operators should establish thresholds for various SS7 message types to ensure that DoS conditions are not created. Also, alarming should be configured to monitor these types of messages to alert when DoS conditions are noted. Rigorous screening procedures can increase the difficulty of launching DDoS attacks. Care must be taken to distinguish DDoS attacks from high volumes of legitimate signaling messages. Maintain backups of signaling element data.

Protect Cellular Service from Anonymous Use

Network Operators and Service Providers should prevent theft of service and anonymous use by enabling strong user authentication as per cellular/wireless standards. Employ fraud detection systems to detect subscriber calling anomalies (e.g., two subscribers using same ID or system access from a single user from widely dispersed geographic areas). In cloning situation remove the ESN to disable user

thus forcing support contact with service provider. Migrate customers away from analog service if possible due to cloning risk.

Protect Cellular Data Channel

Network Operators and Service Providers should encourage the use of IPsec VPN, wireless TLS, or other end-to-end encryption services over the cellular/wireless network. Also, Network Operators should incorporate standards based data encryption services and ensure that such encryption services are enabled for end users. (Data encryption services are cellular/wireless technology specific).

Protect Against Cellular Network Denial of Service

Network Operators should ensure strong separation of data traffic from management/signaling/control traffic, via firewalls. Network operators should ensure strong cellular network backbone security by employing operator authentication, encrypted network management traffic and logging of security events. Network operators should also ensure operating system hardening and up-to-date security patches are applied for all network elements, element management system and management systems.

IR (Incident Response) Procedures

Network Operators and Service Providers should establish a set of standards and procedures for dealing with computer and network security events. These procedures can and should be part of the overall business continuity/disaster recovery plan. Where possible, the procedures should be exercised periodically and revised as needed. Procedures should cover likely threats to those elements of the infrastructure which are critical to service delivery/business continuity.

IR (Incident Response) Team

Network Operators and Service Providers should identify and train a Computer Security Incident Response (CSIRT) Team. This team should have access to the CSO (or functional equivalent) and should be empowered by senior management. The team should include security, networking, and system administration specialists but have the ability to augment itself with expertise from any division of the organization. Organizations that establish part-time CSIRTs should ensure representatives are detailed to the team for a suitable period of time bearing in mind both the costs and benefits of rotating staff through a specialized team.

Incident Response Communications Plan

Network Operators, Service Providers and Equipment Suppliers should develop and practice a communications plan as part of the broader Incident response plan. The communications plan should identify key players and include as a minimum - contact names, business telephone numbers, home tel. numbers, pager numbers, fax numbers, cell phone numbers, home addresses, internet addresses, permanent bridge numbers, etc. Notification plans should be developed prior to an event/incident happening where necessary. The plan should also include alternate

communications channels such as alpha pagers, internet, satellite phones, VOIP, private lines, blackberries, etc. The value of any alternate communications method needs to be balanced against the security and information loss risks introduced.

Intrusion Detection/Prevention Tools (IDS/IPS)

Network Operators and Service Providers should install and actively monitor IDS/IPS tools. Sensor placement should focus on resources critical to the delivery of service.

Intrusion Detection/Prevention Tools (IDS/IPS) Maintenance

Network Operators and Service Providers should maintain and update IDS/IPS tools regularly to detect current threats, exploits, and vulnerabilities.

Intrusion Detection/Prevention (IDS/IPS) Tools Deployment

Network Operators and Service Providers should deploy Intrusion Detection/Prevention Tools with an initial policy that reflects the universe of devices and services known to exist on the monitored network. Due to the ever evolving nature of threats, IDS/IPS tools should be tested regularly and tuned to deliver optimum performance and reduce false positives.

Evidence Collection Guidelines

Network Operators, Service Providers should develop a set of processes detailing evidence collection and preservation guidelines. Procedures should be approved by management/legal counsel. Those responsible for conducting investigations should test the procedures and be trained according to their content. Organizations unable to develop a forensic computing capability should establish a relationship with a trusted third party that possesses a computer forensics capability. Network Administrators and System Administrators should be trained on basic evidence recognition and preservation and should understand the protocol for requesting forensic services.

Threat Awareness

Network Operators and Service Providers should subscribe to vendor patch/security mailing lists to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network.

Denial of Service (DoS) Attack - Target

Where possible, Network Operator's and Service Provider's networks and Equipment Supplier's equipment should be designed to survive significant increases in both packet count and bandwidth utilization. Infrastructure supporting mission critical services should be designed for significant increases in traffic volume and must include network devices capable of filtering and/or rate limiting traffic. Network engineers must understand the capabilities of the devices and how to employ them to maximum effect. Wherever practical, mission critical systems should be deployed in clustered configuration allowing for load balancing of excess

traffic and protected by a purpose built DoS/DDoS protection device. Operators of critical infrastructure should deploy DoS survivable hardware and software whenever possible.

Denial of Service (DoS) Attack - Agent (Zombies)

Network Operators and Service Providers should periodically scan hosts for signs of compromise. Where possible, monitor bandwidth utilization and traffic patterns for signs of anomalous behavior.

Compensating Control for Weak Authentication Methods

For Network Operators and Service Providers legacy systems without adequate access control capabilities, access control lists (ACLs) should be used to restrict which machines can access the device and/or application. In order to provide granular authentication, a bastion host that logs user activities should be used to centralize access to such devices and applications, where feasible.

Protect User IDs and Passwords during Network Transmission

Network Operators, Service Providers and Equipment Suppliers should not send user IDs and passwords in the clear, or send passwords and user IDs in the same message/packet.

Protect Authentication Methods

Network Operators, Service Providers and Equipment Suppliers should develop an enforceable password policy, which considers different types of users, requiring users to protect, as applicable, either (a) the passwords they are given/create or (b) their credentials for two-factor authentication.

Protect Authentication Files and/or Databases

Authentication databases/files used by Network Operators, Service Providers and Equipment Suppliers must be protected from unauthorized access, and must be backed-up and securely stored in case they need to be restored. Filter access to the TCP and/or UDP ports serving the database at the network border. Use strong authentication for those requiring access.

- Prevent users from viewing directory and file names that they are not authorized to access.
- Enforce a policy of least privilege.
- Build a backup system in the event of loss of the primary system. Document and test procedures for backup and restoral of the directory.

Create Trusted PKI Infrastructure When Using Generally Available PKI Solutions

When using digital certificates, Network Operators, Service Providers and Equipment Suppliers should create a valid, trusted PKI infrastructure, using a root certificate from a recognized Certificate Authority or Registration Authority. Assure your devices and applications only accept certificates that were created from a valid PKI infrastructure. Configure your Certificate Authority or Registration Authority to protect it from denial of service attacks.

Expiration of Digital Certificates

For Network Operators, Service Providers and Equipment Suppliers, certificates should have a limited period of validity, dependent upon the risk to the system, and the value of the asset.

If there are existing certificates with unlimited validity periods, and it is impractical to replace certificates, consider the addition of passwords that are required to be changed on a periodic basis.

Define User Access Requirements and Levels

Based on the principles of least-privilege (the minimum access needed to perform the job) and separation of duties (certain users perform certain tasks), Network Operators and Service Providers should develop processes to determine which users require access to a specific device or application. Equipment Suppliers should provide capability to support access levels.

Use Time-Specific Access Restrictions

Network Operators and Service Providers should restrict access to specific time periods for high risk users (e.g., vendors, contractors, etc.) for critical assets (e.g., systems that cannot be accessed outside of specified maintenance windows due to the impact on the business). Assure that all system clocks are synchronized.

Develop Regular Access Audit Procedures

Network Operators, Service Providers and Equipment Suppliers should charter an independent group (outside of the administrators of the devices) to perform regular audits of access and privileges to systems, networks, and applications. The frequency of these audits should depend on the criticality or sensitivity of the associated assets.

Verify Audit Results Through Spot-Checking

Network Operators, Service Providers and Equipment Suppliers should validate any regular auditing activity through spot-checking to validate the competency, thoroughness, and credibility of those regular audits.

Promptly Address Audit Findings

Network Operators, Service Providers and Equipment Suppliers should promptly verify and address audit findings assigning an urgency and priority commensurate with their implied risk to the business. The findings as well as regular updates to those findings should be reported to management responsible for the affected area.

Conduct Risk Assessments to Determine Appropriate Security Controls

Network Operators, Service Providers and Equipment Suppliers should perform a risk assessment of all systems and classify them by the value they have to the company and the impact to the company if they are compromised or lost. Based on the risk assessment, develop a security policy which recommends and assigns the appropriate controls to protect the system.

Restrict Use of Dynamic Port Allocation Protocols

Network Operators, Service Providers and Equipment Suppliers should restrict dynamic port allocation protocols such as Remote Procedure Calls (RPC) and some classes of Voice-over-IP protocols (among others) from usage, especially on mission critical assets, to prevent host vulnerabilities to code execution. Dynamic port allocation protocols should not be exposed to the internet. If used, such protocols should be protected via a dynamic port knowledgeable filtering firewall or other similar network protection methodology.

Strong Encryption for Customer Clients

Service Providers should implement customer client software that uses the strongest permissible encryption appropriate to the asset being protected.

Training for Security Staff

Network Operators, Service Providers and Equipment Suppliers should establish security training programs and requirements for ensuring security staff knowledge and compliance. This training could include professional certifications in ICT security.

Conduct Organization Wide Security Awareness Training

Network Operators, Service Providers and Equipment Suppliers should ensure staff is given awareness training on security policies, standards, procedures, and general best practices. Awareness training should also cover the threats to the confidentiality, integrity, and availability of data including social engineering. Training as part of new employee orientation should be supplemented with regular "refreshers" to all staff.

Staff Training on Technical Products and Their Controls

To remain current with the various security controls employed by different technologies, Network Operators, Service Providers and Equipment Suppliers should ensure that technical staff participate in ongoing training and remain up-to-

date on their certifications for those technologies. Staff Trained on Incident Reporting: Network Operators, Service Providers and Equipment Suppliers should provide procedures and training to staff on the reporting of security incidents, weaknesses, and suspicious events.

Document and Verify All Security Operational Procedures

Network Operators and Service Providers should ensure that all security operational procedures, system processes, and security controls are documented, and that documentation is up to date and accessible by appropriate staff. Perform gap analysis/audit of security operational procedures as often as security policy requires relative to the asset being protected. Using results of analysis or audit, determine which procedures, processes, or controls need to be updated and documented.

Proper Wireless LAN/MAN Configurations

Network Operators and Service Providers should secure Wireless WAN/LAN networks sufficiently to ensure that a) monitoring of RF signals cannot lead to the obtaining of proprietary network operations information or customer traffic and that b) Network access is credibly authenticated.

Protection of Cellular User Voice Traffic

Network Operators and Service Providers should incorporate cellular voice encryption services and ensure that such encryption services are enabled for end users. (Voice encryption services depend on the wireless technology used, and are standards based).

Authentication System Failure

In the event of an authentication system failure, Network Operators and Service Providers should determine how the system requiring support of the authentication system responds (i.e., determine what specific effect(s) the failure caused). The system can either be set to open or closed in the event of a failure. This will depend on the needs of the organization. For instance, an authentication system supporting physical access should be required to fail OPEN in the event of a failure so people will not be trapped in the event of an emergency. However, an authentication system that supports electronic access to core routers should be required to fail CLOSED to prevent general access to the routers in the event of authentication system failure. In addition, it is important to have a means of alternate authenticated access to a system in the event of a failure. In the case of core routers failing CLOSED, there should be a secondary means of authentication (e.g., use of a one-time password) reserved for use only in such an event; this password should be protected and only accessible to a small key-contingent of personnel.

Automated Patch Distribution Systems

Network Operators, Service Providers and Equipment Suppliers should ensure that patching distribution hosts properly sign all patches. Critical systems must only use

OSs and applications which employ automated patching mechanisms, rejecting unsigned patches.

Protect Sensitive Data in Transit for Externally Accessible Applications

Network Operators and Service Providers should encrypt sensitive data from web servers, and other externally accessible applications, while it is in transit over any networks they do not physically control.

Protect Management of Externally Accessible Systems

Network Operators and Service Providers should protect the systems configuration information and management interfaces for Web servers and other externally accessible applications, so that it is not inadvertently made available to 3rd parties. Techniques, at a minimum, should include least privilege for external access, strong authentication, application platform hardening, and system auditing.

SNMP Community String Vulnerability Mitigation

Service Providers, Network Operators, and Equipment Suppliers should use difficult to guess community string names, or current SNMP version equivalent. Mitigate Control Plane Protocol Vulnerabilities in Suppliers Equipment. Suppliers should provide controls to protect network elements and their control plane interfaces against compromise and corruption. Vendors should make such controls and filters easy to manage and minimal performance impacting. Participate in Industry Forums to Improve Control Plane Protocols Network Operators, Service Providers and Equipment Suppliers should participate in industry forums to define secure, authenticated control plane protocols and operational, business processes to implement them.

Handle Policy Violations Consistently

Network Operators, Service Providers and Equipment Suppliers should handle violations of policy in a manner that is consistent, and, depending on the nature of the violation, sufficient to either deter or prevent a recurrence. There should be mechanisms for ensuring this consistency.

Consistent Security Controls for DR Configurations

A Network Operator's or Service Provider's disaster recovery or business continuity solutions should adhere to the same Information Security best practices as the solutions used under normal operating conditions.

Security-Related Data Analysis

Network Operators and Service Providers should review and analyze security-related event data produced by critical systems on a regular basis to identify potential security risks and issues. Automated tools and scripts can aid in this analysis process and significantly reduce the level of effort required to perform this review.

7. Network Elements (NEs) Security Guidelines :

IDENTIFICATION

- Within specific NE, the NE should enforce unambiguous User-IDs to identify its users.
- All NE interfaces and ports that accept user command inputs should require unambiguous User-ID before performing any actions.
- The NE should internally maintain the identity of all current active users.
- The NE should restrict a User-ID to only one active session.
- All operations-related processes running on the NE should be associated with the User-ID of the invoking user.
- If a user-ID has not been used for a specified time interval, the NE should be capable of disabling that User-ID. In addition, the security administrator should have a choice of automatic or manual disabling of these User-IDs.

AUTHENTICATION

- The NE shall verify the identity of all users prior to allowing access.
- All NE interfaces and ports that accept user command inputs shall require user authentication before performing any actions.
- The NE shall ensure the confidentiality of all internally stored authentication data and protect it from access by unauthorized users.
- Reusable passwords transmitted across networks, including wireless or other unprotected channels, shall be encrypted.
- The NE shall preserve the confidentiality and integrity of stored authentication information such as passwords, PINs, and authentication tokens.
- Authentication information entered during login shall be immediately overwritten within the NE.
- The NE shall not permit users to bypass the authentication mechanism.
- Only designated security administrators shall be able to access protected authentication information.
- The NE shall prohibit the outputting or writing of a clear text representation of authentication information to any printer, terminal, or data entry device.
- The NE shall perform the entire authentication procedure even if an invalid User-ID is entered. The NE shall not disclose which part of the

authentication is incorrect and shall provide no information to the user other than "invalid attempt."

- The NE shall require users to change passwords after a specified period of time. Users shall be prevented from choosing a password that they have previously used until a specified period of time elapses.
- The NE should require those users who access the system remotely to use an authentication mechanism stronger than a password.
- Users who perform critical administrative and other OAM&P functions should be authenticated by means of a procedure that is stronger than passwords; for example, a biometrics, token-based, or cryptographic technique.

SYSTEM ACCESS CONTROL

- The NE shall not allow access to any user unless identified and authenticated. Only authorized users, processes or remote systems shall be allowed access.
- All ports and interfaces of the NE that accept operations-related command inputs shall exercise access control. This includes ports that provide direct, dial-up, and data communications network access.
- The NE shall not allow any session to be established via a port that is not designed to accept operations-related command inputs.
- The NE shall not provide any default User-IDs that can permit unauthenticated system access.
- The NE log-in procedure shall exit and end the session if the user authentication procedure is incorrectly performed a specified number of times. This value shall be set by the security administrator.
- Exceeding the threshold for incorrectly performing the user authentication procedure shall be considered a security relevant event. The NE shall notify the security administrator in real time of this occurrence.
- When the threshold for incorrectly performing the user identification procedure has been exceeded, the NE shall lock out that log-in port for a specified interval of time.
- To prevent unauthorized users from purposely locking out all input ports by performing incorrect user authentications, the default lock-out period shall not exceed 60 seconds. Only the security administrator shall be able to modify that value.
- When the threshold for incorrectly performing the user authentication procedure has been exceeded, the NE shall not suspend the associated User-ID. Suspension could allow an unauthorized user to disable all accounts.
- When a logical connection is established, but before access, the NE shall provide an advisory warning message regarding unauthorized

entry/use and its possible consequences. The message shall comply with applicable local, state, and federal laws.

- Upon successful access to the NE, the system shall display for the user the date and time of the user's last successful access to the NE and the number of unsuccessful attempts.
- The NE shall automatically disconnect a user and require reauthentication after a specified period of inactivity. The time-out interval shall be set by the security administrator.
- The NE shall end a session by means of a secure log-off procedure. The port shall be dropped immediately if the session is interrupted due to causes such as time-out, power failure, link disconnection, etc.
- The NE shall be able to incorporate and support mechanisms to grant or deny access to any user based on time-of-day, day-of-week, and calendar date.

RESOURCE ACCESS CONTROL

- The NE shall provide a level of granularity such that for each user allowed access to resources it shall be possible to grant access rights to specific software, processes, databases, data, etc.
- Only authorized users shall be allowed access to software in the NE. Software shall be access controlled for overwrite and update, as well as execution rights.
- Control of access to resources shall be based on authenticated user identification.
- The NE shall have the capability to screen access to specified resources and restrict a user's ability to perform certain designated operations on the basis of originating address/port. Unauthorized addresses/ports shall be denied access.
- Modification of the access rights to a resource shall be allowed only by the owner of that resource or by an appropriate security administrator.
- The NE shall provide a mechanism to remove access rights to all resources for a user or a group of users.
- The NE shall protect the data files and tables associated with the access control mechanisms from unauthorized access.
- Users having predefined roles shall not have default rights to modify their roles and associated rights.

DATA AND SYSTEM INTEGRITY

- The NE shall have the capability to identify the original creator of any named or user-accessible NE resources such as data and processes.
- The NE shall have the capability to identify the originator of any operations information received via communications networks.

- The NE shall provide mechanisms that allow it to periodically validate its correct operation.
- The NE shall have the capability to protect the integrity of stored data by performing cryptographically-based integrity checks (e.g., message authentication code) and/or data updates.
- The NE shall be designed and developed to protect data integrity by checking inputs for reasonable values.
- Documentation for the NE shall contain recommendations for running, on a regular basis, integrity checking utilities for file systems and disks.
- A non-privileged user action, either deliberate or accidental, that requests NE resources shall not cause denial of service of the NE to other users.
- Mechanisms shall be provided to allow the NE to recover from a failure or discontinuity without risk of compromising security.
- To facilitate recovery, and to reduce the potential impact of a security compromise, check points shall be included in the software.
- The NE shall provide mechanisms to preserve the integrity of data stored internally to the NE.
- The NE shall have the capability to verify the integrity of new software releases and subsequent patches.
- The NE shall process security alarms in real-time based on indicated severity levels.

AUDIT

- The NE shall generate logs that contain information about security relevant events. Items selected for recording shall be defined and selected by the security administrator. The logs shall enable security administrators to investigate losses and improper actions on the part of users, legitimate and otherwise, and to seek legal remedies.
- The NE shall provide audit capabilities with user accountability for all significant events. The user-identification associated with any request or activity shall be maintained and passed on to any other connected systems so that the initiating user can be traceable for the lifetime of the request or activity.
- The audit log shall be protected from unauthorized access or destruction by means of access controls based on user and channel privileges.
- The audit log and audit control mechanisms shall be protected from modification or destruction.
- The audit log and audit control mechanisms shall survive system restarts by being maintained throughout a system restart.

- The security administrator shall be immediately notified if the audit log fails to record the events that are required to be recorded.
- It shall not be possible to disable the audit log of actions taken by a security administrator.
- Authentication information such as passwords, PINs, and cryptographic keys shall not be recorded in the security log.
- In order to prevent overwriting any information, the NE shall be capable of automatically forwarding the audit log to a storage device or authorized management system. Any transmission of audit information shall be done securely.
- When the audit log is copied to other media or locations, the copy shall start at the oldest record and copy sequentially without deleting any records.
- The NE shall support audit analysis tools that can produce exception reports, summary reports, and detailed reports on specific data items, users, or communication facilities.

SECURITY ADMINISTRATION

- The NE shall separate administrator functions from other user functions. Only authorized security administrators shall be allowed to execute these functions.
- The security functions performed by authorized administrators shall be identified and documented.
- The NE shall provide a mechanism for an authorized administrator to display all currently active users or software processes. These processes include both OAM&P and telecommunications service applications.
- The NE shall provide a mechanism for an authorized administrator to be able to independently and selectively review the action of any one or more users, including privileged users, based on individual user identity.
- The NE shall provide a mechanism that permits an authorized administrator to monitor the activities of a specific terminal, port or network address in real time.
- The NE shall provide a mechanism to allow an authorized administrator to lock out a specific port or channel.
- The NE shall provide a mechanism to allow an authorized administrator to authorize or revoke users.
- The NE shall provide a mechanism to allow an authorized administrator to identify all resources owned by or accessible to any specific user along with the associated access privileges.
- The NE shall provide a mechanism to allow an authorized administrator to create a unique User-ID for a particular user.

- The NE shall provide a mechanism to allow an authorized administrator to disable User-IDs after a specified period of time during which the user-ID has not been used.
- The NE shall provide a mechanism to allow an authorized administrator to reinstate or delete a disabled User-ID.
- The NE shall provide a mechanism to allow an authorized administrator to enter, reset, or delete passwords for users.
- An authorized administrator shall not be able to retrieve any password in clear text.
- The NE shall provide the capability to generate alarms for specifiable security events. The alarms shall be prioritized based on pre-determined criteria and routed to the security administrator. Only an authorized security administrator can deactivate an alarm.
- The NE shall provide a mechanism to allow an authorized administrator to periodically validate the correct operation of the NE with respect to the supported applications.

DATA CONFIDENTIALITY

- The type of data items and structures whose confidentiality is protected shall be identified. For example, if data is transmitted, some identifier might accompany the transaction which would identify the key and related attributes needed by the receiving system.
- The system shall have the capability of protecting the confidentiality of each individual message or selective fields of each message.
- The NE shall support mechanisms that ensure the confidentiality of communication information by encryption if the communication media cannot be protected by physical and administrative means.

8. Recovery Guidelines:

Recovery from Digital Certificate Key Compromise

In the event the key in a digital certificate becomes compromised, Network Operators, Service Providers and Equipment Suppliers should immediately revoke the certificate, and issue a new one to the users and/or devices requiring it. Perform Forensics and Post-mortem, as prescribed in NRIC BP 8061, to review for additional compromise as soon as business processes allow.

Recovery from Root Key Compromise

In the event the root key in a digital certificate becomes compromised, Network Operators, Service Providers and Equipment Suppliers should secure a new root key, and rebuild the PKI (Public Key Infrastructure) trust model. Perform Forensics and Post-mortem, as prescribed in NRIC BP 8061, to review for additional compromise as soon as business processes allow.

Recovery from Vulnerable or Unnecessary Services

When a compromise occurs, or new exploits are discovered, Network Operators and Service Providers should perform an audit of available network services to reassess any vulnerability to attack and re-evaluate the business need to provide that service, or explore alternate means of providing the same capability.

Recovery from Encryption Key Compromise or Algorithm Failure

When improper use of keys or encryption algorithms is discovered, or a breach has occurred, Network Operators and Service Providers should conduct a forensic analysis to assess the possibility of having potentially compromised data and identify what may have been compromised and for how long it has been in a compromised state; implement new key (and revoke old key if applicable), or encryption algorithm, and ensure they are standards-based and implemented in accordance with prescribed procedures of that standard, where possible. When using wireless systems, ensure WEP (Wireless Encryption Privacy) and WP2 (Wireless Privacy) vulnerabilities are mitigated with proper security measures.

Roll-out of Secure Service Configuration, or Vulnerability Recovery Configurations

When new default settings introduce vulnerabilities or the default configuration is found to be vulnerable, Network Operators and Service Providers should work with the Equipment Supplier to resolve the inadequacies of the solution, using a pre-deployment, staging area, where hardened configurations can be tested.

Document Single Points of Failure during Recovery

Following a compromise and reestablishment of lost service, Network Operators and Service Providers should re-evaluate the architecture for single points of failure

(SPOF). Review the process of evaluating and documenting single points of failure and provide spares for redundancy in the architecture to ensure adequacy of the security architecture.

Enforce Least-Privilege-Required Access Levels during Recovery

When it is discovered that a system is running with a higher level of privilege than necessary, Network Operators and Service Providers should consider which systems/services the affected system could be disconnected from to minimize access and connectivity while allowing desired activities to continue; conduct a forensic analysis to assess the possibility of having potentially compromised data and identify what may have been compromised and for how long it has been in a compromised state; and reconnect system to back-office with appropriate security levels implemented.

Post-Mortem Review of Security Architecture after Recovery

Immediately following incident recovery, Network Operators and Service Providers should re-evaluate the adequacy of existing security architecture and implement revisions as needed. Ensure any changes are adequately documented to reflect the current configuration. Review existing processes for establishing and maintaining security architectures update as necessary to maintain currency.

Recover from Poor Network Isolation and Partitioning

When, through audit or incident, a co-mingling of data or violation of a trust relationship is discovered, Network Operators and Service Providers should, as part of a post-mortem process, review segmentation design to evaluate adequacy of the architecture and data isolation.

Recover from Compromise of Sensitive Information Stored on Network Systems/Elements

When compromise or trust violations occur, Network Operators and Service Providers and Equipment Suppliers should conduct a forensic analysis to determine the extent of compromise, revoke compromised keys, and establish new crypto keys as soon as possible, and review crypto procedures to re-establish trust.

Recovery from Not having and Enforcing an Acceptable Use Policy

In the event that an Acceptable Use Policy is not in place, or an event occurs that is not documented within the AUP, Network Operators and Service Providers should consult with legal counsel. Consulting with legal counsel, develop and adapt a policy based on lessons learned in the security incident and redistribute the policy when there are changes.

Recovery from Network Misuse via Invalid Source Addresses

Upon discovering the misuse or unauthorized use of the network, Service Providers should shut down the port in accordance with AUP (Acceptable Use Policy) and

clearance from legal counsel. Review ACL (Access Control List) and temporarily remove offending address pending legal review and reactivate the port.

Recovery from Misuse or Undue Consumption of System Resources

If a misuse or unauthorized use of a system is detected, Network Operators and Service Providers should perform forensic analysis on the system, conduct a post-mortem analysis and establish system resource quotas.

Recovery from Unauthorized Information Dissemination

If information has been leaked or the release policy has not been followed, Network Operators, Service Providers and Equipment Suppliers should review audit trails; Change passwords, review permissions, and perform forensics as needed; inform others at potential risk for similar exposure; and include security responsibilities in performance improvement programs that may include security awareness refresher training.

Recover from Failure of Hiring Procedures

When it is discovered that there has been a failure in the hiring process and the new employee does not in fact have the proper capabilities or qualifications for the job, Network Operators, Service Providers and Equipment Suppliers should undertake one or more of the following: 1) Provide additional employee training. 2) Reassign, dismiss, or discipline the employee.

Recover from Misuse of Equipment for Remote Access of Corporate Resources

In the event of misuse or unauthorized use in a remote access situation contrary to the AUP (Acceptable Use Policy), Network Operators and Service Providers should terminate the VPN (Virtual Private Network) connection and issue a warning in accordance with the employee code of conduct. If repeated, revoke employee VPN remote access privileges.

Recover from Discovery of Unsanctioned Devices on the Organizational Network

Upon discovery of an unsanctioned device on the organizational network, Network Operators and Service Providers should investigate to determine ownership and purpose/use of the device. Where possible, this phase should be non-alerting (i.e. log reviews, monitoring of network traffic, review of abuse complaints for suspect IP address) to determine if the use is non-malicious or malicious/suspect. If use is determined to be non-malicious, employ available administrative tools to correct behavior and educate user.

Recovery from Network Element Resource Saturation Attack

If the control plane is under attack, Network Operators and Service Providers should: 1) Turn on logging and analyze the logs, 2) Implement the appropriate filter and access list to discard the attack traffic 3) Utilize DoS/DDoS tracking methods to identify the source of attack.

Recovery from BGP (Border Gateway Protocol) Poisoning

If the routing table is under attack from malicious BGP updates, Network Operators and Service Providers should apply the same filtering methods used in NRIC BP 8043 more aggressively to stop the attack. When under attack, the attack vector is usually known and the performance impacts of the filter are less of an issue than when preventing an attack. The malicious routes will expire from the table, be replaced by legitimate updates, or in emergencies, can be manually deleted from the tables. Contact peering partner to coordinate response to attack.

Recover from Interior Routing Table Corruption

If the interior routing has been corrupted, Network Operators and Service Providers should implement policies that filter routes imported into the routing table. The same filtering methods used in NRIC 8045 can be applied more aggressively. The malicious routes will expire from the table, be replaced by legitimate updates, or in emergencies, can be manually deleted from the tables. If needed, the authentication mechanism/crypto keys between IGP neighbors should also be changed.

Recover from Compromised DNS (Domain Name System) Servers or Name Record Corruption

If the DNS (Domain Name System) server has been compromised or the name records corrupted, Network Operators and Service Providers should implement the pre-defined disaster recovery plan. Elements may include but are not limited to: 1) bring-on additional hot or cold spare capacity, 2) bring up a known good DNS server from scratch on different hardware, 3) Reload and reboot machine to a know good DNS server software (from bootable CD or spare hard drive), 4) Reload name resolution records from a trusted back-up. After the DNS is again working, conduct a post-mortem of the attack/response.

Recover from MPLS (Multi-Protocol Label Switching) Mis-configuration

If a customer MPLS-enabled trusted VPN (Virtual Private Network) has been compromised by mis-configuration of the router configuration, Network Operators and Service Providers should 1) restore customer specific routing configuration from a trusted copy, 2) notify customer of potential security breach, 3) Conduct an investigation and forensic analysis to understand the source, impact and possible preventative measures for the security breach.

Recover from SCP Compromise

No prescribed standard procedures exist for Network Operators and Service Providers to follow after the compromise of an SCP (Signaling Control Point). It will depend on the situation and the compromise mechanism. However, in a severe case, it may be necessary to disconnect it to force a traffic reroute, then revert to known-good, back-up tape/disk and cold boot.

Recover from SS7 DoS Attack

If an SS7 Denial of Service (DoS) attack is detected, Network Operators and Service Providers should more aggressively apply the same thresh holding and filtering mechanism used to prevent an attack (NRIC BP 8053). The alert/alarm will specify the target of the attack. Isolate, contain and, if possible, physically disconnect the attacker. If necessary, isolate the targeted network element and disconnect to force traffic reroute.

Recover from Anonymous SS7 Use

If logs or alarms determine an SS7 table has been modified without proper authorization, Network Operators and Service Providers should remove invalid records, or in the event of a modification, rollback to last valid version of record. Investigate the attack to identify required security changes.

Recover from Cellular Service Anonymous Use or Theft of Service

If anonymous use or theft of service is discovered, Network Operators and Service Providers should 1) disable service for attacker, 2) Involve law enforcement as appropriate, since anonymous use is often a platform for crime. If possible, triangulate client to identify and disable. If the wireless client was cloned, remove the ESN (Electronic Serial Number) to disable user thus forcing support contact with service provider.

Recover from Cellular Network Denial of Service Attack

If the attack is IP based, Network Operators and Service Providers should reconfigure the Gateway General Packet Radio Service Support Node (GGSN) to temporarily drop all connection requests from the source. Another approach is to enforce priority tagging. Triangulate the source(s) to identify and disable. (It is easier to recover from a cellular network denial of service attack if the network is engineered with redundancy and spare capacity).

Recover from Unauthorized Remote OAM&P Access

When an unauthorized remote access to an OAM&P system occurs, Network Operators and Service Providers should consider terminating all current remote access, limiting access to the system console, or other tightened security access methods. Continue recovery by re-establishing new passwords, reloading software, running change detection software, or other methods, continuing quarantine until recovery is validated, as practical.

Lack of Business Recovery Plan

When a Business Recovery Plan (BRP) does not exist, Network Operators and Service Providers should bring together an ad-hoc team to address the current incident. The team should have technical, operations, legal, and public relations representation. Team should be sponsored by senior management and have a direct communication path back to management sponsor. If situation exceeds internal

capabilities consider contracting response/recovery options to 3rd party security provider.

Evidence Collection Procedures during Recovery

Insomuch as is possible without disrupting operational recovery, Network Operators and Service Providers should handle and collect information as part of a computer security investigation in accordance with a set of generally accepted evidence-handling procedures.

Recovery from the Absence of a Monitoring Requests Policy

In the absence of a monitoring request polity, Network Operators and Service Providers should refer all communications intercept requests to corporate counsel.

Recovery from Lack of Security Reporting Contacts

If an abuse incident occurs without reporting contacts in place, Network Operators and Service Providers should: 1) Ensure that the public-facing support staff is knowledgeable of how both to report incidents internally and to respond to outside inquiries. 2) Ensure public facing support staff (i.e. call/response center staff) understands the security referral and escalation procedures. 3) Disseminate security contacts to industry groups/coordination bodies where appropriate. 4) Create e-mail IDs per rfc2142 and disseminate.

Recovery from Lack of IDS/IPS Maintenance

In the event of a security threat, Network Operators and Service Providers should upload current IDS/IPS signatures from vendors and re-verify stored data with the updated signatures. Evaluate platform's ability to deliver service in the face of evolving threats and consider upgrade/replacement as appropriate. Review Incident Response Post-Mortem Checklist (NRIC BP 8564).

Recovery from Denial of Service Attack - Target

If a network element or server is under DoS attack, Network Operators and Service Providers should evaluate the network and ensure the issue is not related to a configuration/hardware issue. Determine direction of traffic and work with distant end to stop inbound traffic. Consider adding more local capacity (bandwidth or servers) to the attacked service. Where available, deploy DoS/ DDoS specific mitigation devices and/or use anti-DoS capabilities in local hardware. Coordinate with HW vendors for guidance on optimal device configuration. Where possible, capture hostile code and make available to organizations such as US-CERT and NCS/NCC for review.

Recovery from Denial of Service Attack - Equipment Vulnerability

When a denial of service vulnerability or exploit is discovered, Equipment Suppliers should work with clients to ensure devices are optimally configured. Where possible, analyze hostile traffic for product improvement or mitigation/response options, disseminate results of analysis.

Recovery from Authentication System Failure

In the event an authentication system fails, Network Operators, Service Providers and Equipment Suppliers should make sure the system being supported by the authentication system is in a state best suited for this failure condition. If the authentication system is supporting physical access, the most appropriate state may be for all doors that lead to outside access be unlocked. If the authentication system supporting electronic access to core routers fails, the most appropriate state may be for all access to core routers be prohibited.

9. Physical Security Guidelines:

- Network Operators, Service Providers and Property Managers should post emergency contact number(s) and unique site identification in an externally visible location at unmanned communication facilities (e.g., towers, cell sites, Controlled Environment Vault (CEV), satellite earth stations). This signage should not reveal additional information about the facility, except when necessary.
- Property Managers should consider maintaining a list of authorized climbers and a log of authorized tower climbs.
- Network Operators and Property Managers should have agreements in place to ensure necessary and timely access to cell sites.
- Network Operators, Service Providers and Equipment Suppliers should, where programs exist, coordinate with local, state and/or federal emergency management and law enforcement agencies for pre-credentialing to help facilitate access by technicians to restricted areas during an event.
- Network Operators, Service Providers and Property Managers should perform periodic inspections of fire and water stopping where cable ways pass through floors and walls (e.g., sealing compounds).
- Network Operators, Service Providers, Equipment Suppliers, and Property Managers should develop a comprehensive Site Management and/or Building Certification Program to ensure that every critical equipment location has carefully documented procedures to ensure fire safety. These procedures should include, among other things, guidance for the safe operation of all electrical appliances at this facility, including space heaters which are a frequent source of fires.
- Network Operators and Service Providers and Property Managers should secure remote power maintenance systems to prevent unauthorized use.

- Network Operators, Service Providers and Equipment Suppliers should conduct and periodically re-validate physical security assessments on critical network facilities.

- Network Operators, Service Providers and Equipment Suppliers should establish additional access control measures that provide two factor identification (e.g., cameras, PIN, biometrics) in conjunction with basic physical access control procedures at areas of critical infrastructure, as appropriate, to adequately protect the assets.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop and implement periodic physical inspections and maintenance as required for all critical security systems.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit compliance with physical security policies and procedures.

- Network Operators, Service Providers and Equipment Suppliers should conduct electronic surveillance (e.g., CCTV, access control logs, alarm monitoring) at critical access points.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should have policies and procedures that address tailgating (i.e. following an authorized user through a doorway or vehicle gateway). At critical sites, consider designing access points to minimize tailgating.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that access control records are retained in conjunction with company standards.

- Network Operators, Service Providers and Equipment Suppliers should deploy security measures in proportion to the criticality of the facility or area being served.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should alarm and monitor critical facility access points to detect intrusion or unsecured access (e.g., doors being propped open).

- Network Operators, Service Providers and Equipment Suppliers should limit access to areas of critical infrastructure to essential personnel.

- In facilities where master key systems are used, Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing hierarchical key control system(s) (e.g., Master Key Control systems) with record keeping data bases and implemented so that keys are

distributed only to those with need for access into the locked space (e.g., perimeter doors, offices, restricted areas).

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and maintain inventory control measures to protect all media associated with Master Key Control (MKC) systems and access control systems.

- Network Operators, Service Providers and Equipment Suppliers should establish separation policies and procedures that require the return of all corporate property and invalidate access to all corporate resources (physical and logical) to coincide with the separation of employees, contractors and vendors.

- Network Operators, Service Providers and Equipment Suppliers should consider establishing corporate standards and practices to drive enterprise-wide access control to a single card and single system architecture to mitigate the security risks associated with administering and servicing multiple platforms.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and enforce access control and identification procedures for all individuals (including visitors, contractors, and vendors) that provide for the issuing of ID badges, and the sign-in and escorting procedures where appropriate.

- Network Operators, Service Providers and Equipment Suppliers should internally identify and document areas of critical infrastructure as part of security and emergency response planning. This documentation should be kept current and protected as highly sensitive proprietary information.

- Network Operators, Service Providers and Equipment Suppliers should establish and enforce a policy that requires all individuals to properly display company identification (e.g., photo ID, visitor badge) while on company property. Individuals not properly displaying a badge should be challenged and/or reported to security.

- Network Operators, Service Providers and Equipment Suppliers should include security as an integral part of the strategic business planning and decision making process to ensure that security risks are properly identified and appropriately mitigated.

- Network Operators, Service Providers and Equipment Suppliers should include security as an integral part of the merger, acquisition and divestiture process to ensure that security risks are proactively identified and appropriate plans are developed to facilitate the integration and migration of organizational functions (e.g., Due Diligence investigations, integration of policy and procedures).

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should include security as an integral part of the facility construction process to ensure that security risks are proactively identified and appropriate solutions are included in the design of the facility. Where appropriate, this review may include elements such as facility location selection, security system design, configuration of the lobby, limitation of outside access points (both doors and windows), location of mailroom, compartmentalization of loading docks, design of parking setbacks, placement and protection of air handling systems and air intakes, structural enhancements, and ramming protection. Consider sign off authority for security and safety on all construction projects.

- Security and Human Resources (for Network Operators, Service Providers or Equipment Suppliers) should partner on major issues to ensure that security risks are identified and plans are developed to protect the company's personnel and assets (e.g., hiring, downsizing, outsourcing, labor disputes, civil disorder).

- Network Operators, Service Providers and Equipment Suppliers should establish policies and procedures related to access control to provide exception access (e.g., emergency repair or response, forgotten credential, etc.).

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should facilitate the availability of security related hardware and media (e.g., spare hardware) and/or a contingency plan for its availability in the event of a disaster.

- Network Operators, Service Providers and Equipment Suppliers should provide a level of security protection over critical inventory (i.e., spares) that is proportionate to the criticality of the equipment.

- Network Operators, Service Providers and Equipment Suppliers should establish a role for the security function (i.e., physical and cyber) in business continuity planning, including emergency response plans and periodic tests of such plans.

- Network Operators, Service Providers and Equipment Suppliers should establish a procedure governing the assignment of facility access levels.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing and implementing background investigation policies that include criminal background checks of employees. The policy should detail elements of the background investigation as well as disqualification criteria.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing contractual obligations requiring contractors, subcontractors and vendors to conduct background investigations of all personnel who require unescorted access to areas of critical infrastructure or who require access to sensitive information related to critical infrastructure.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should install environmental emergency response equipment (e.g., fire extinguishers, high rate automatically activated pumps) where appropriate, and periodically inspect the equipment.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and implement policies and procedures to secure and restrict access to power, environmental, security, and fire protection systems.

- Network Operators, Service Providers and Property Managers should establish and implement policies and procedures to secure and restrict access to fuel supplies.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should comply with security standards for perimeter lighting.

- Network Operators, Service Providers, Equipment Suppliers or Property Managers should plan and maintain landscaping at facilities to enhance the overall level of building security wherever possible. Landscaping at critical facilities should not obstruct necessary security lighting or camera views of ingress and egress areas, and landscaping should also avoid creating fire hazards or hiding places.

- Network Operators and Property Managers should ensure critical infrastructure utility vaults are secured from unauthorized access.

- Network Operators, Service Providers and Equipment Suppliers should establish and implement a policy that requires approval by senior member(s) of the security department for security related goods and services contracts.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider a strategy of using technology (e.g., access control, CCTV, sensor technology, person traps, turnstiles) to supplement the guard force.

- When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers and Property Managers, a supervision plan should be established that requires supervisory checks for all posts.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers using guard services should ensure that each post has written detailed post orders including site specific instructions, up to date emergency contact information and ensure that on the job training occurs.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should periodically audit guard services to ensure satisfactory performance, and compliance with organizational contractual requirements.

- When guard services are utilized by Network Operators, Service Providers, Equipment Suppliers or Property Managers, a process should be developed to quickly disseminate information to all guard posts. This process should be documented and should clearly establish specific roles and responsibilities.

- Network Operators, Service Providers and Equipment Suppliers should establish and maintain (or contract for) a 24/7 emergency call center for internal communications. Ensure staff at this center has access to all documentation pertinent to emergency response and up to date call lists to notify appropriate personnel. The number to this call center should be appropriately published so personnel know where to report information.

- Back-up Power: Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).

- Network Operators, Service Providers and Equipment Suppliers should staff critical functions at appropriate levels, considering human factors such as workload and fatigue.

- Network Operators, Service Providers and Equipment Suppliers should make security an ongoing priority and provide periodic, at least annually, security awareness information to all personnel. Where appropriate, include contractors and other regular visitors.

- Network Operators, Service Providers and Property Managers should establish standards, policies and procedures that, where feasible, separate Inter-connector equipment and personnel access from ILEC floor space.

- For Network Operators, Service Providers collocation sites, the Property Manager should require all tenants to adhere to the security standards set for that site.

- In order to prepare for contingencies, Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.

- Network Operators, Service Providers and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis. Assessments should address natural disasters and unintentional or intentional acts of people on facility or nearby structures.

- Network Operators, Service Providers, and Equipment Suppliers should document in a Disaster Recovery Plan the process for restoring physical security control points for critical infrastructure facilities.

- Network Operators and Service Providers should be automatically notified upon the loss of alarm data and react accordingly.

- Equipment Suppliers should ensure appropriate physical security controls are designed and tested into new products and product upgrades (e.g., tamper resistant enclosures).

- Service Providers, Network Operators and Equipment Suppliers should establish, implement and enforce appropriate procedures for the storage and movement of equipment and material, including trash removal, to deter theft.

- Network Operators, Service Providers and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.

- Network Operators, Service Providers and Equipment Suppliers should establish an incident reporting mechanism and investigations program so that security or safety related events are recorded, analyzed, and investigated as appropriate.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should implement a tiered security response plan for communications facilities that recognizes the threat levels identified in the Homeland Security Advisory System.

- Network Operators, Service Providers and Equipment Suppliers should require compliance with corporate security standards and programs for contractors, vendors and others, as appropriate. This requirement should be included as part of the terms and conditions of the contract that the contractor or vendor has with the company, and should also be made to apply to their subcontractors.

- Network Operators, Service Providers and Equipment Suppliers should establish and implement corporate security standards and requirements in consideration of the best practices of the communications industry (e.g., NRIC Best Practices).

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider keeping centralized trash collection outside the building to reduce the potential for fire and access to the building. Dumpsters should be located away from the buildings where feasible.

- Network Operators and Equipment Suppliers should consider the security implications of equipment movement both domestically and internationally, including movement across borders and through ports of entry.

- Equipment Suppliers should consider participating in and complying with an industry organization that develops standards in their security, logistics and transportation practices.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish, implement and enforce mailroom and delivery procedures that recognize changes in threat conditions.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide and reinforce as appropriate mail screening procedures to relevant employees and contractors to increase attention to security.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should provide periodic briefings and/or make available industry/Government guidance for identifying suspicious letters or parcels, to personnel (employees or contractors) involved in shipping, receiving or mailroom activities at major locations or critical sites. Protocols for handling any suspicious items should be established in advance and implemented upon the receipt of any suspicious letter or parcel.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should evaluate the potential benefits and security implications when making decisions about building and facility signage, both internally and externally.

- Network Operators, Service Providers and Equipment Suppliers should develop and consistently implement software delivery procedures that protect the integrity of the delivered software in order to prevent software loads from being compromised during the delivery process.

- Network Operators should provide appropriate security for emergency mobile trailers (both pre- and post-deployment) in order to protect against a coordinated terrorist attack on emergency communications capabilities.

- Network Operators, Service Providers and Equipment Suppliers should consider establishing a policy to manage the risks associated with key personnel traveling together.

- Network Operators, Service Providers and Equipment Suppliers should consider restricting, supervising, and/or prohibiting tours of critical network facilities, systems and operations.

- Network Operators, Service Providers and Property Managers located in the same facility should coordinate security matters and include all tenants in the overall security and safety notification procedures, as appropriate.

- Network Operators, Service Providers and Equipment Suppliers should consider performing targeted sweeps of critical infrastructures and network operations centers for listening devices when suspicion warrants.

- Network Operators, Service Providers and Equipment Suppliers should consider unannounced internal security audits at random intervals to enforce compliance with company security policies.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing procedures for video equipment and recording, where utilized (e.g., storage, accurate time/date stamping and regular operational performance checks).

- Network Operators, Service Providers and Equipment Suppliers should establish and enforce a policy to immediately report stolen or missing company vehicles and trailers to the appropriate authorities.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should utilize a coordinated physical security methodology that incorporates diverse layers of security in direct proportion to the criticality of the site.

- Network Operators, Service Providers and Equipment Suppliers should establish a proprietary information protection policy to protect proprietary information in their possession belonging to the company, business partners and customers from inadvertent, improper or unlawful disclosure. The policy should establish procedures for the classification and marking of information; storage, handling, transfer and transmission of information as well as the destruction of information.

- Network Operators, Service Providers and Equipment Suppliers should establish policies and procedures that mitigate workplace violence.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure the inclusion of fire stair returns in their physical security designs. Further, they should ensure that there are no fire tower or stair re-entries into areas of critical infrastructure, where permitted by code.

- Property Managers of collocation and telecom hotel facilities should be responsible and accountable for common space, critical shared areas (e.g., cable vault, power sources) and perimeter security for the building with consideration of industry standards and best practices.

- Network Operators and Service Providers in multi-tenant communications facilities (e.g., telecom hotels) should provide or arrange security for their own space with consideration of NRIC Best Practices and in coordination with the existing security programs for the building.

- Network Operators, Service Providers that are tenants within telecom hotels should plan accordingly to protect their own facilities from potential risks within

the building complex (e.g., fire suppression system, plumbing, hazardous materials).

- Network Operators and Service Providers tenants of a telecom hotel should provide a current list of all persons authorized for access to the Property Manager, provide periodic updates to this list, and provide instructions for exceptions (e.g., emergency restoration personnel).

- Network Operators and Service Providers should provide appropriate protection for outside plant equipment (e.g., Controlled Environmental Vault, remote terminals) against tampering and should consider monitoring certain locations against intrusion.

- Network Operators, Service Providers and Property Managers should restrict access to the AC transfer switch housing area, ensure that scheduled maintenance of the transfer switch is performed, and ensure that spare parts are available.

- Network Operators, Service Providers and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.

- Network Operators, Service Providers and Property Managers should, where feasible, place fuel tanks in a secured and protected area. Access to fill pipes, fuel lines, vents, etc. should be restricted (e.g., containment by fencing, walls, buildings, buried) to reduce the possibility of unauthorized access.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should raise awareness of appropriate personnel regarding possible secondary events immediately after an incident and promptly report any suspicious conditions.

- Network Operators, Service Providers and Equipment Suppliers who utilize foreign sites should establish and implement a comprehensive physical security program for protecting corporate assets, including personnel, at those sites.

- Network Operators, Service Providers and Equipment Suppliers should consider limiting the dissemination of information relating to future locations of key leadership.

- Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.

- Network Operators, Service Providers and Equipment Suppliers should verify proper functioning of electronic surveillance equipment (e.g., CCTV, access control logs, alarm monitoring) at critical access points after any incident that may impact such equipment.

- Network Operators, Service Providers and Property Managers should provide or arrange for security to protect temporary equipment placements and staging areas for critical infrastructure equipment in a disaster area.

- Network Operators, Service Providers and Equipment Suppliers should ensure that impacted alarms and monitors associated with critical utility vaults are operational after a disaster event.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should have a provision for responding to malfunctioning access control equipment.

- Network Operators, Service Providers and Equipment Suppliers should consider placing access and facility alarm points to critical or sensitive areas on backup power.

- Network Operators, Service Providers and Equipment Suppliers should restrict visits and tours at the affected areas during the restoration period following a major incident.

- Network Operators, Service Providers and Equipment Suppliers should make all employees, contractors, and others with access to critical infrastructure during restoration aware of changes to security posture resulting from the incident, and increased vigilance should be encouraged.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should take into account failed security systems after an event when determining restoration priorities.

- Network Operators, Service Providers and Equipment Suppliers should define and assign responsibility for retrieval of all corporate assets (e.g., access cards, equipment) and ensure temporary physical and logical access is removed after completion of a restoration effort for all temporary personnel associated with the restoration.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should establish and enforce access control and identification procedures for all individuals (including temporary contractors, and mutual aid workers) at restoration sites for which they have responsibility. Provide for issuing and proper displaying of ID badges and the sign-in and escorting procedures, where appropriate.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should brief affected personnel involved in a restoration on any significant changes to access control procedures.

- Network Operators', Service Providers', Equipment Suppliers' and Property Managers' senior management should actively support compliance with established corporate security policies and procedures.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should incorporate various types of diversionary tactics into exercises to assess the security response.

- Network Operators, Service Providers and Equipment Suppliers should include security considerations in disaster recovery plans for critical infrastructure sites.

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should, in facilities using automated access control systems, install one mechanical lock to permit key override access to the space(s) secured by the access control system in the event the system fails in the locked mode. An appropriate procedure should be followed to track and control the keys.

- Network Operators, Service Providers and Equipment Suppliers who develop hardware, software or firmware should ensure that appropriate security programs are in place for protecting the product from theft or industrial espionage, taking into consideration that some developmental environments around the world present a higher risk level than others.

- Network Operators, Service Providers and Equipment Suppliers should consider site specific (e.g., location, region, country) threat information during security program development.

- Network Operators, Service Providers and Equipment Suppliers should instruct security personnel to confirm the authenticity of directions to supersede existing security processes or procedures.

10. Reference Security Standards & Best Practices

- **Network Reliability and Interoperability Council**
  - NRIC Best Practices (www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm)
- **Alliance for Telecommunication Industry Solutions ATIS/ANSI**
  - T1.276-2003: Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane ARP Spoofing
  - NIIF 5029: NIIF Reference Document Part X- Attachment A- Security Guidelines: January, 2004
  - T1.268-2000: Telecommunications Management Network - Public Key Infrastructure - Digital Certificates and Certificate Revocations Lists.
- **ITU**
  - Handbook on Security in Telecommunications and Information Technology
  - X.800 Security architecture for Open Systems Interconnection for CCITT applications
  - X.802 Information technology - Lower layers security model
  - X.803 Information technology - Open Systems Interconnection - Upper layers security model
  - X.805 Security architecture for systems providing end-to-end communications
  - X.810 Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview
  - X.811 Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework

- X.812 Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework
- X.813 Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework
- X.814 Information technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework
- X.815 Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework
- X.816 Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework
- Y.2701 – Security Requirements for NGN Release 1

- **Telcordia**

  - GR-815-CORE - Generic Requirements for Network Element/Network System Security - March 2002
  - SR-Notes-Series - 19 -Telcordia Notes on Public Switched Network (PSN) Security - 2002/06/3
  - GR-1194 - Bellcore Operations Systems Security Requirements - December 1998
  - GR-1332-CORE - Generic Requirements for Data Communications Network Security - 1996/04/01
  - GR-1253-CORE -Generic Requirements for Operations Interfaces Using OSI Tools: Telecommunications Management Network Security Administration - 1995/06/01
  - GR-1469-CORE -Generic Requirements on Security for OSI-Based Telecommunications Management Network Interface (A Module of OTGR FR-439) - 1995/12/01
  - GR-3025-Core - Generic Requirements for Security of Public Key Infrastructure (PKI) Supporting Telecommunications Management Network (TMN) - 2001/07/01

- GR-3026-Core - Generic Requirements for Security for SNMP-Based Telecommunications Management Network (TMN) Interfaces - 2001/10/01

- **National Institute of Standards and Technology (NIST)**
  - NIST Special Publications
  - The National Information Assurance Partnership(NIAP) Program Common Criteria
  - Federal Information Processing Standards (FIPS)
- **IEEE**
  - 802.1X-2001 - IEEE standard for local and metropolitan area networks - Port-based network access control
  - IEEE 1363-2000 - IEEE Standard Specifications for Public Key Cryptography
- **ISO**
  - ISO 7498-2:1989 - Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture
  - ISO 17799-2005 - Information technology. Code of practice for information security management. (BS7799)
- **Optical Internetworking Forum**
  - Security for Management Interfaces to Network Elements - Sept 2003
  - Security Extension for UNI and NNI - May 2003 IEEE 1363-2000
- **ATM Forum**
  - af-sec-0096.000 - ATM Security Framework Version 1.0 - February, 1998
  - af-sec-0100.001 - ATM Security Specification Version 1.0 - Feb, 1999
  - af-sec-0100.002 - ATM Security Specification Version 1.1 - March, 2001

- af-sec-0163.000.pdf - Security Specification Version 1.1 Protocol Implementation Conformance Statement (PICS) Performa Specification -March, 2001
- af-sec-0172.pdf - Control Plane Security -Nov, 2001
- af-sec-0179.000 - Methods of Securely Managing ATM Network Elements implementation Agreements, Version 1.1 - April, 2002
- sec-0180.000 - Security Services Renegotiation Addendum to Security, Version 1.1 - af-March, 2002
- af-sec-0187.000 - Addendum to Security Specification v1.1 - In-Band Security for Simplex Connections - August, 2002
- af-sec-0189.000 - Addendum to Sec 1.1 Secure CBR Traffic in a Policed Network - July, 2002

- **SANS (SysAdmin, Audit, Network, Security)**
  - The SANS Security Policy (http://www.sans.org/resources/policies/)

List of Acronyms

ICT	Information & Communication Technology
SPOF	Single point of failure
CIDR	Classless Inter-Domain Routing
QoS	Quality of Service
OAM&P	Operations, Administration, Management, and Provisioning
DoS	Denial of service
DDoS	Distributed Denial of Service
SS7	Signaling System 7
ACL	Access Control Lists
AUP	Acceptable Use Policy
SCP	Signaling Control Point