

NRIC Best Practices Result

Network Type(s): Internet/Data

Industry Role(s): Service Provider

Keyword(s): Cyber Security

204 Best Practices are found.

*Press Best Practice number to get detailed information.

Number	Description
7-5-0524	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.
7-5-0526	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.
7-6-0763	Service Providers implementing DNS servers in support of VoIP applications such as ENUM should provision those servers per the IETF Best Current Practices for operation of DNS nameservers: BCP 40 (RFC 2182) and BCP 16 (RFC 2870).
7-6-0764	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.
7-6-0767	Service Providers implementing a SIP-signaled VoIP network should consider using media gateway controllers according to IETF RFC 3372 BCP 63, Session Initiation Protocol for Telephones (SIP-T): Context and Architectures, in order to achieve interoperability with SS7/ISUP-signaled TDM voice networks.
7-6-0768	Service Providers implementing a SIP-signaled VoIP network should consider using media gateway controllers that map ISUP-to-SIP and SIP-to-ISUP messages according to IETF RFC 3398, Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping in order to achieve a consistent interpretation of ISUP-to-SIP messaging industrywide.
7-6-0769	Service Providers implementing a BICC-signaled network should consider implementing ITU-T Recommendation Q.1912.5, Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control Protocol or ISDN User Part, or 3GPP TS 29.163, Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks, to achieve interoperability between an SS7/ISUPsignaled TDM voice network and a

	SIP-signaled VoIP network.
7-6-0770	Wireless Service Providers who have deployed IS-41 or GSM Mobility Application Part (MAP) signaling networks should consider implementing and using the network management controls of SS7 within their networks.
7-6-0810	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.
7-6-0811	Service Providers should make available meaningful information about expected performance with respect to upstream and downstream throughput and any limitations of the service. Specified rate services (such as those covered by QoS or similar systems) should be handled by an SLA between the parties.
7-6-5162	Network Operators, Service Providers and Equipment Suppliers should ensure adequate physical protection for facilities/areas that are used to house certificates and/or encryption key management systems, information or operations.
7-6-5165	Network Operators, Service Providers and Equipment Suppliers should ensure that teleworkers (e.g., remote software developers) have the equipment and support necessary to secure their computing platforms and systems to the equivalent level of those on-site. Security software, firewalls and locked file cabinets are all considerations.
7-6-5170	Network Operators, Service Providers and Equipment Suppliers should control or disable all administrative access ports (e.g., manufacturer) into R&D or production systems (e.g., remap access ports, require callback verification, add second level access gateway).
7-6-8011	Request OAM&P Security Features: Service Providers and Network Operators should request products from vendors that meet current industry baseline requirements for Operations, Administration, Management, and Provisioning (OAM&P) security.
7-6-8012	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. Examples of trusted paths that might adequately protect the OAM&P communications include separate private-line networks, VPNs or encrypted tunnels. Any sensitive OAM&P traffic that is mixed with customer traffic should be encrypted. OAM&P communication via TFTP and Telnet is acceptable if the communication path is secured by the carrier. OAM&P traffic to customer premises equipment should also be via a trusted path.
7-6-8013	Controls for Operations, Administration, Management, and Provisioning (OAM&P) Management Actions: Network Operators and Service Providers should authenticate, authorize, attribute, and log all management actions on critical infrastructure elements and management systems. This especially applies to management actions involving security resources such as passwords, encryption keys, access control lists, time-out values, etc.
7-6-8014	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.

7-6-8015	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.
7-6-8016	OAM&P Security Architecture: Network Operators and Service Providers should design and deploy an Operations, Administration, Management, and Provisioning (OAM&P) security architecture based on industry recommendations.
7-6-8017	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.
7-6-8021	Switched Hubs for OAM&P Networks: In critical networks for Operations, Administration, Management, and Provisioning (OAM&P), Network Operators, Service Providers and Equipment Suppliers should use switched network hubs so that devices in promiscuous mode are less likely to be able to see/spoof all of the traffic on that network segment.
7-6-8023	Scanning Operations, Administration, Management and Provisioning (OAM&P) Infrastructure: Network Operators and Service Providers should regularly scan infrastructure for vulnerabilities/exploitable conditions. Operators should understand the operating systems and applications deployed on their network and keep abreast of vulnerabilities, exploits, and patches.
7-6-8028	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.
7-6-8032	Patching Practices: Network Operators, Service Providers and Equipment Suppliers should design and deploy a patching process based on industry recommendations, especially for critical OAM&P systems.
7-6-8035	Software Patch Testing: The patch/fix policy and process used by Network Operators and Service Providers should include steps to appropriately test all patches/fixes in a test environment prior to distribution into the production environment.
7-6-8036	Exceptions to Patching: Network Operators and Service Providers systems that are not compliant with the patching policy should be noted and these particular elements should be monitored on a regular basis. These exceptions should factor heavily into the organization's monitoring strategy. Vulnerability mitigation plans should be developed and implemented in lieu of the patches. If no acceptable mitigation exists, the risks should be communicated to management.
7-6-8037	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.
7-6-8038	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.
7-6-8039	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.
7-6-8043	Prevent BGP (Border Gateway Protocol) Poisoning: Network Operators and Service Providers should use existing BGP filters to avoid propagating incorrect data. Options include: 1) Avoid route flapping DoS by implementing RIPE-229 to minimize the dampening risk to critical resources, 2) Stop malicious routing table growth due to de-aggregation by implementing Max-Prefix Limit on peering connections, 3) Employ ISP filters to permit customers to only advertise IP address blocks assigned to them, 4) Avoid disruption to networks that use documented special use addresses by ingress and egress filtering for Martian routes, 5) Avoid DoS caused by unauthorized route injection (particularly from compromised customers) by egress filtering (to peers) and ingress filtering (from customers) prefixes set to other ISPs, 6) Stop DoS from unallocated 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 7) Employ Murphy filter (guarded trustand mutual suspicion) to reinforce filtering your peer should have done.
7-6-8044	BGP (Border Gateway Protocol) Interoperability Testing: Network Operators and Service Providers should conduct configuration inter-operability testing during peering link set-up; Encourage Equipment Suppliers participation in interoperability testing forums and funded test-beds to discover BGP implementation bugs.
7-6-8047	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: 1) increase DNS resiliency through redundancy and robust network connections 2) Have separate name servers for internal and external traffic as well as critical infrastructure, such as OAM&P and signaling/control networks 3) Where feasible, separate proxy servers from authoritative name servers 4) 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.
7-6-8048	Protect DNS (Domain Name System) from Poisoning: Network Operators, Service Providers and Equipment Suppliers should mitigate the possibility of DNS cache poisoning by using techniques such as 1) Preventing recursive queries 2) Configure short (2 day) Time-To-Live for cached data 3) Periodically refresh or verify DNS name server configuration data and parent pointer records. Service Providers, Network Operators, and Equipment Suppliers should participate in forums to define an operational implementation of DNSSEC.
7-6-8049	Protect DHCP (Dynamic Host Configuration Protocol) Server from Poisoning: Network Operators and Service Providers should employ techniques to make it difficult to send unauthorized DHCP information to customers and the DHCP servers themselves. Methods can include OS Hardening, router filters, VLAN configuration, or encrypted, authenticated tunnels. The DHCP servers themselves must be hardened, as well. Mission critical applications should be assigned static addresses to protect against DHCP-based denial of service attacks.
7-6-	MPLS (Multi-Protocol Label Switching) Configuration Security: Network Operators and

8050	Service Providers should protect the MPLS router configuration by 1) Securing machines that control login, monitoring, authentication and logging to/from routing and monitoring devices 2) Monitoring the integrity of customer specific router configuration provisioning 3) Implementing (e)BGP filtering to protect against labeled-path poisoning from customers/peers.
7-6-8066	Sharing Information with Industry & Government: Network Operators, Service Providers and Equipment Suppliers should participate in regional and national information sharing groups such as the National Coordinating Center for Telecommunications (NCC), Telecom-ISAC (Information Sharing and Analysis Center), and the ISP-ISAC (when chartered), Network Security Information Exchange (NSIE), and the National Infrastructure Protection Center (NIPC). Formal membership and participation will enhance the receipt of timely threat information and will provide a forum for response and coordination. Membership will also afford access to proprietary threat and vulnerability information (under NDA) that may precede public release of similar data. Because of the critical nature of this information, 24x7 coverage should be considered.
7-6-8069	Monitoring Requests: Network Operators, Service Providers and Equipment Suppliers should identify a Point of Contact (POC) for handling requests for the installation of lawfully approved intercept devices. Once a request is reviewed and validated, the primary POC should serve to coordinate the installation of any monitoring device with the appropriate legal and technical staffs.
7-6-8071	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.
7-6-8078	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.
7-6-8087	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.
7-6-8090	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.
7-6-8093	Validate Source Addresses: Service Providers should validate the source address of all traffic sent from the customer for which they provide Internet access service and block any traffic that does not comply with expected source addresses. Service Providers typically assign customers addresses from their own address space, or if the customer has their own address space, the service provider can ask for these address ranges at provisioning. (Network Operators may not be able to comply with this practice on links to upstream/downstream providers or peering links, since the valid source address space is not known).
7-6-	Strong Encryption for Customer Clients: Service Providers should implement customer client

8094	software that uses the strongest permissible encryption appropriate to the asset being protected.
7-6-8096	Users Should Employ Protective Measures: Network Operators and Service Providers should educate service customers on the importance of, and the methods for, installing and using a suite of protective measures (e.g., strong passwords, anti-virus software, firewalls, IDS, encryption) and update as available.
7-6-8101	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.
7-6-8102	Discourage Use of Personal Equipment for Corporate Activities: Network Operators, Service Providers and Equipment Suppliers should discourage the use of personal equipment for telecommuting, virtual office, remote administration, etc.
7-7-0401	Network Surveillance: Network Operators and Service Providers should monitor the network to enable quick response to network issues.
7-7-0402	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).
7-7-0408	Ingress Filtering: Network Operators and Service Providers should, where feasible, implement RFC 3704 (IETF BCP84) ingress filtering.
7-7-0409	Routing Resiliency: 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.
7-7-0410	Security Services and Procedures: Network Operators and Service Providers should, as appropriate, review, understand, and implement Internet Service Provider Security Services and Procedures (RFC3013/BCP46).
7-7-0412	IP Element Security: To enhance security, Network Operators and Services Providers should, by default, disable ICMP (Internet Control Message Protocol) redirect messages and IP source routing.
7-7-0428	Software & Hardware Vulnerability Tracking: 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 and CERTs (Computer Emergency Response Teams).
7-7-0437	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.
7-7-0438	CIDR Use: Network Operators and Service Providers should enable CIDR (Classless Inter-Domain Routing) by implementing classless route prefixes on routing elements.
7-7-0439	BGP Authentication: Network Operators and Service Providers should authenticate BGP sessions (e.g., using TCP MD5) with their own customers and other providers.
7-7-0440	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 misconfigurations.
7-7-0441	Unicast RPF: Network Operators and Service Providers should, where feasible, implement Unicast RPF (Reverse Path Forwarding) to help minimize DOS attacks that use source address spoofing.
7-7-0442	End-to-End Path Monitoring: Service Providers should consider measuring end-to-end path performance and path validity for both active and alternate routes.
7-7-0449	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.
7-7-0507	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).
7-7-0515	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.
7-7-0516	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.
7-7-0520	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.
7-7-0546	Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).
7-7-0617	Route Controls: Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions.
7-7-0766	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 voiceband communication (e.g., DTMF tones, facsimile, TTY/TDD).
7-7-0779	Network Operators, Service Providers and Equipment Suppliers should establish a means to allow for coordination between cyber and physical security teams supporting preparedness, response, investigation and analysis.
7-7-0804	Service Providers should consider appropriate means for providing their customers with information about their traffic policies so that users may be informed when planning and utilizing their applications.
7-7-	Service Providers, Network Operators and Equipment Suppliers should work to establish

0805	operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless).
7-7-0808	Release Filtering Information/Policies to Customers: Network Operators and Service Providers should make information available to customers about traffic filtering (both static and dynamic), where required by law.
7-7-0816	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).
7-7-1026	Network Operators and Service Providers should consider creating a corporate policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.
7-7-5070	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 cyber security.
7-7-5227	Network Operators, Service Providers, Equipment Suppliers and Property Managers should perform after-action reviews of emergency response and restoration of major events to capture lessons learned (e.g., early warning signs) and to enhance emergency response and restoration plans accordingly. A process similar to NRIC Appendix Z Recovery Incident Response (IR) Post Mortem Checklist can be used to capture and identify countermeasures to prevent or mitigate the impact of future incidents and to quickly and effectively restore service from such events in the future.
7-7-5267	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that operating procedures are clearly defined, and followed by personnel during emergency situations in order to avoid degradation of cyber and physical security due to a diversion.
7-7-5270	Network Operators, Service Providers, Equipment Suppliers and Property Managers personnel should be aware that terrorists or malicious groups may use false information to cause heightened public or employee awareness to divert attention and resources to other areas away from their intended physical or cyber target. Where feasible, information (e.g., news sources, e-mail) should be authenticated and cross-verified to ensure accuracy of information.
7-7-5271	Network Operators and Service Providers should consider physical and cyber security issues in Mutual Aid Agreements (e.g., authorization, access control, badging).
7-7-5276	Network Operators, Service Providers and Equipment Suppliers that use networked electronic access control systems should apply appropriate security and reliability principles for critical systems (e.g., cyber security).
7-7-8000	Disable Unnecessary Services: Network Operators and Service Providers should establish a process, during design/implementation of any network/service element or management system, to identify potentially vulnerable, network-accessible services (such as Network Time Protocol (NTP), Remote Procedure Calls (RPC), Finger, Rsh-type commands, etc.) and either disable, if unneeded, or provided additional external network protection, such as proxy servers, firewalls, or router filter lists, if such services are required for a business purpose.
7-7-8001	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 3DES or AES.
7-7-8003	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.
7-7-8005	Document Single Points of Failure: Network Operators and Service Providers should implement a continuous engineering process to identify and record single points of failure (SPOF) and any components that are critical to the continuity of the infrastructure. The process should then pursue architectural solutions to mitigate the identified risks as appropriate.
7-7-8006	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.
7-7-8007	Define Security Architecture(s): Network Operators and Service Providers should develop formal written Security Architecture(s) and make the architecture(s) readily accessible to systems administrators and security staff for use during threat response. The Security Architecture(s) should anticipate and be conducive to business continuity plans.
7-7-8008	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.
7-7-8018	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.
7-7-8019	Hardening OSs for OAM&P: Network Operators, Service Providers and Equipment Suppliers with devices equipped with operating systems used for OAM&P should have operating system hardening procedures applied. Hardening procedures include (a) all unnecessary services are disabled; (b) all unnecessary communications pathways are disabled; (c) all critical security patches have been evaluated for installations on said systems/applications; and d) review and implement published hardening guidelines, as appropriate. Where critical security patches cannot be applied, compensating controls should be implemented.
7-7-8020	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 affect on network and component devices.
7-7-8022	Remote Operations, Administration, Management and Provisioning (OAM&P) Access: Network Operators and Service Providers should have a process by which there is a risk assessment and formal approval for all external connections. All such connections should be individually identified and restricted by controls such as strong authentication, firewalls, limited methods of connection, and fine-grained access controls (e.g., granting access to only specified parts of an application). The remote party's access should be governed by contractual controls that ensure the provider's right to monitor access, defines appropriate use of the access, and calls for adherence to best practices by the remote party.
7-7-8024	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.
7-7-8025	Protection from SCADA Networks: Telecom/Datacomm OAM&P networks for Network Operators and Service Providers should be isolated from other OAM&P networks, e.g., SCADA networks, such as for power, water, industrial plants, pipelines, etc. <ul style="list-style-type: none"> • Isolate the SCADA network from the OAM&P network (segmentation) • Put a highly restrictive device, such as a firewall, as a front-end interface on the SCADA network for management access. • Use an encrypted or a trusted path for the OAM&P network to communicate with the SCADA "front-end."
7-7-8026	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.
7-7-8027	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.
7-7-8029	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: <ul style="list-style-type: none"> • 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.

7-7-8030	OAM&P Session Times: For Network Operators and Service Providers and Equipment Suppliers, all OAM&P applications, systems, and interfaces should use session timers to disconnect, terminate, or logout authenticated sessions that remain inactive past some preset (but ideally configurable by the Administrator) time limit that is appropriate for operational efficiency and security.
7-7-8031	LAES Interfaces and Processes: Network Operators, Service Providers and Equipment Suppliers should develop and communicate Lawfully Authorized Electronic Surveillance (LAES) policy. They should: <ul style="list-style-type: none"> • Limit the distribution of information about LAES interfaces • Periodically conduct risk assessments of LAES procedures • Audit LAES events for policy compliance • Limit access to those who are authorized for LAES administrative functions or for captured or intercepted LAES content • Promote awareness of all LAES policies among authorized individuals.
7-7-8033	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.
7-7-8034	Software Patching Policy: Network Operators and Service Providers should define and incorporate a formal patch/fix policy into the organization's security policies.
7-7-8040	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.
7-7-8042	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 by applying techniques such as: 1) eBGP hop-count (TTL) limit to end of physical peering link, 2) MD5 session signature to mitigate route update spoofing threats (keys should be changed periodically where feasible).
7-7-8046	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.
7-7-8061	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. See Appendix X and Y.
7-7-8062	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.
7-7-8063	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.
7-7-8064	Security-Related Data Collection Network Operators and Service Providers should generate and collect security-related event data for critical systems (i.e. syslogs, firewall logs, IDS alerts, remote access logs, etc.). Where practical, this data should be transmitted to secure collectors for storage and should be retained in accordance with a data retention policy. A mechanism should be enabled on these systems to ensure accurate timestamps of this data (e.g., Network Time Protocol).
7-7-8065	Sharing Information with Law Enforcement: Network Operators, Service Providers and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities and identify a single Point of Contact (POC) for coordination/referral activities.
7-7-8067	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.
7-7-8068	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.
7-7-8070	Abuse Reporting: Network Operators and Service Providers should have Abuse Policies and processes posted for customers (and others), instructing them where and how to report instances of service abuse. Service Providers, Network Operators, and Equipment Suppliers should support the email IDs listed in rfc 2142 "MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS."

7-7-8072	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.
7-7-8073	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.
7-7-8074	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.
7-7-8075	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.
7-7-8077	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.
7-7-8079	Use Strong Passwords: Network Operators, Service Providers and Equipment Suppliers should create an enforceable policy that considers different types of users and requires the use of passwords or stronger authentication methods. Where passwords can be used to enhance needed access controls, ensure they are sufficiently long and complex to defy brute-force guessing and deter password cracking. To assure compliance, perform regular audits of passwords on at least a sampling of the systems.
7-7-8080	Change Passwords on a Periodic Basis: Network Operators, Service Providers and Equipment Suppliers should change passwords on a periodic basis implementing a policy which considers different types of users and how often passwords should be changed. Perform regular audits on passwords, including privileged passwords, on system and network devices. If available, activate features across the user base which force password changes.
7-7-8081	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.
7-7-8083	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

	<p>restored.</p> <p>Filter access to the TCP and/or UDP ports serving the database at the network border. Use strong authentication for those requiring access.</p> <p>Prevent users from viewing directory and file names that they are not authorized to access.</p> <p>Enforce a policy of least privilege.</p> <p>Build a backup system in the event of loss of the primary system. Document and test procedures for backup and restoral of the directory.</p>
7-7-8084	<p>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.</p>
7-7-8085	<p>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.</p> <p>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.</p>
7-7-8086	<p>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.</p>
7-7-8088	<p>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.</p>
7-7-8089	<p>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.</p> <p>Based on the risk assessment, develop a security policy which recommends and assigns the appropriate controls to protect the system.</p>
7-7-8091	<p>Protect Cached Security Material: Network Operators, Service Providers and Equipment Suppliers should evaluate cache expiration and timeouts of security material (such as cryptographic keys and passwords) to minimize exposure in case of compromise. Cached security material should be immediately deleted from the cache when the cached security material expires.</p>
7-7-8092	<p>Adopt and Enforce Acceptable Use Policy: Network Operators and Service Providers should adopt a customer-directed policy whereby misuse of the network would lead to measured enforcement actions up to and including termination of services.</p>
7-7-	<p>Establish System Resource Quotas: Network Operators and Service Providers should establish,</p>

8095	where technology allows, limiters to prevent undue consumption of system resources (e.g., system memory, disk space, CPU consumption, network bandwidth) in order to prevent degradation or disruption of performance of services.
7-7-8097	Create Policy on Information Dissemination: Network Operators, Service Providers and Equipment Suppliers should create an enforceable policy clearly defining who can disseminate information, and what controls should be in place for the dissemination of such information. The policy should differentiate according to the sensitivity or criticality of the information.
7-7-8098	Create Policy on Removal of Access Privileges: Network Operators, Service Providers and Equipment Suppliers should have policies on changes to and removal of access privileges upon staff members status changes such as terminations, exits, transfers, and those related to discipline or marginal performance.
7-7-8099	Create Policy on Personnel Hiring Merits: Network Operators, Service Providers and Equipment Suppliers should perform background checks that are consistent with the sensitivity of the position's responsibilities and that align with HR policy. These checks could include those that verify employment history, education, experience, certification, and criminal history.
7-7-8100	Training for Cyber 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 cyber security.
7-7-8103	Protect Network/Management Infrastructure from Malware: Network Operators and Service Providers should deploy malware protection tools where feasible, establish processes to keep signatures current, and establish procedures for reacting to an infection.
7-7-8104	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.
7-7-8106	Protect 3G Cellular from Cyber Security Vulnerabilities: Network Operators, Service Providers and Equipment Suppliers should employ operating system hardening and up-to-date security patches for all accessible wireless servers and wireless clients. Employ strong end user authentication for wireless IP connections. Employ logging of all wireless IP connections to ensure traceability back to end user. In particular, vulnerable network and personal data in cellular clients must be protected if the handset is stolen. Apply good IP hygiene principles.
7-7-8108	<p>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 may 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 may be required to fail CLOSED to prevent general access to the routers in the event of authentication system failure.</p> <p>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</p>

	event; this password should be protected and only accessible to a small key-contingent of personnel.
7-7-8109	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.
7-7-8110	News Disinformation: Information from news sources may be spoofed, faked, or manipulated by potential attackers. Network Operators, Service Providers and Equipment Suppliers should ensure news sources are authenticated and cross-verified to ensure accuracy of information, especially when not from a trusted source.
7-7-8111	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.
7-7-8112	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.
7-7-8113	Limited Local Logon: Network Operators, Service Providers and Equipment Suppliers should not permit local logon of users other than the system administrator. Local logon of a system administrator should be used only as a last resort.
7-7-8114	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.
7-7-8116	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.
7-7-8117	DNS Servers Disaster Recovery Plan: Network Operators and Service Providers should prepare a disaster recovery plan to implement upon DNS server compromise.
7-7-8118	Protect Against DNS (Domain Name System) Distributed Denial of Service: Network Operators and Service Providers should provide DNS DDoS protection by implementing protection techniques such as: 1) Rate limiting DNS network connections 2) Provide robust DNS capacity in excess of maximum network connection traffic 3) Have traffic anomaly detection and response capability 4) Provide secondary DNS for back-up 5) Deploy Intrusion Prevention System in front of DNS.
7-7-8119	Security-Related Data Correlation Network Operators and Service Providers should correlate data from various sources, including non-security related sources, (i.e. syslogs, firewall logs, IDS alerts, remote access logs, asset management databases, human resources information, physical access logs, etc.) to identify security risks and issues across the enterprise.
7-7-8120	Revocation of Digital Certificates Network Operators, Service Providers and Equipment Suppliers should use equipment and products that support a central revocation list and revoke certificates that are suspected of having been compromised.

7-7-8121	Conduct Regular Audits of Information Security Practices: Network Operators, Service Providers and Equipment Suppliers should conduct regular audits of their Information Security practices.
7-7-8123	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.
7-7-8124	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.
7-7-8125	Policy Acknowledgement: Network Operators, Service Providers and Equipment Suppliers should ensure that employees formally acknowledge their obligation to comply with their corporate Information Security policies.
7-7-8126	Use Risk-Appropriate Authentication Methods: Network Operators, Service Providers and Equipment Suppliers should employ authentication methods commensurate with the business risk of unauthorized access to the given network, application, or system. For example, these methods would range from single-factor authentication (e.g., passwords) to two-factor authentication (e.g., token and PIN) depending on the estimated criticality or sensitivity of the protected assets. When two-factor authentication generates one-time passwords, the valid time-duration should be determined based on an assessment of risk to the protected asset(s).
7-7-8127	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.
7-7-8128	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.
7-7-8129	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.
7-7-8130	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.
7-7-8131	Include Security Incidents in Business Recovery Plan: A Network Operator's or Service Provider's Business Recovery Plan should factor in potential Information Security threats of a plausible likelihood or significant business impact.
7-7-8132	Leverage Business Impact Analysis for Incident Response Planning: Network Operators and Service Providers should leverage the Business Continuity Planning/Disaster Recovery (BCP/DR) Business Impact Assessment (BIA) efforts as input to prioritizing and planning Information and/or Physical Security Incident Response efforts.

7-7-8133	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.
7-7-8136	Protect Network/Management Infrastructure from Unexpected File System Changes: Network Operators and Service Providers should deploy tools to detect unexpected changes to file systems on Network Elements and Management Infrastructure systems, where feasible, and establish procedures for reacting to changes. Use techniques such as cryptographic hashes.
7-7-8138	Renewal of Digital Certificates Network Operators, Service Providers and Equipment Suppliers should establish a procedure to track the expiration date for digital certificates used in services and critical applications, and start the process to renew such certificates in sufficient time to prevent disruption of service.
7-7-8139	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.
7-7-8500	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.
7-7-8501	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.
7-7-8502	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.
7-7-8503	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.
7-7-8505	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.
7-7-	Document Single Points of Failure During Recovery: Following a compromise and

8506	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.
7-7-8507	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.
7-7-8508	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.
7-7-8509	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.
7-7-8510	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.
7-7-8513	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.
7-7-8514	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.
7-7-8515	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.
7-7-8517	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.
7-7-8519	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.
7-7-8521	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.
7-7-8522	<p>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.</p> <p>If use is determined to be non-malicious, employ available administrative tools to correct behavior and educate user. Conduct review of policies to determine:</p> <ol style="list-style-type: none"> 1. If additional staff education regarding acceptable use of network/computing resources is required. 2. If processes should be redesigned / additional assets allocated to provide a sanctioned replacement of the capability. Was the user attempting to overcome the absence of a legitimate and necessary service the organization was not currently providing so that s/he could perform their job? <p>If the use is deemed malicious/suspect, coordinate with legal counsel:</p> <ol style="list-style-type: none"> 1. Based on counsel's advice, consider collecting additional data for the purposes of assessing the risk to the organization and the scope of any potential damages. Options may include additional network monitoring, remote scanning of system, remote access to any publicly accessible services (i.e. web/ftp). 2. Depending on the scope of the misuse, consider a referral to law enforcement. <ol style="list-style-type: none"> 2.a If matter is referred to law enforcement, cooperate as required. 3. If matter is not referred to law enforcement, prepare to confront user. <ol style="list-style-type: none"> 3.a. Depending on severity of the issue, arrange for permanent/temporary suspension of system access. 3.b. Confront user regarding personnel/HR policies. Ensure user does not have access to network or suspect system at the time of confrontation. 3.c. Disconnect system from network before allowing user access. 3.d. Request permission to examine system (see evidence/forensic procedures section if permission is granted). 3.e. If permission to review system is denied, follow-up with Legal/HR about the disposition of the device. 3.f. Follow HR procedures regarding disciplinary actions. 4. Conduct review of policies to determine: <ol style="list-style-type: none"> 4.a. If additional staff education regarding acceptable use of network/computing resources

	isrequired 4.b. If security monitoring and awareness procedures adequately protect organization.
7-7-8523	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.
7-7-8525	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.
7-7-8526	Recover from Interior Routing Table Corruption: If the interior routing has been corrupted, Network Operators and Service Providers should implement policies that filters 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.
7-7-8527	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.
7-7-8528	Recover from DNS (Domain Name System) Denial of Service Attack: If the DNS server is under attack, Network Operators and Service Providers should consider one or more of the following steps 1) Implement reactive filtering to discard identified attack traffic, if possible, 2) Rate-limiting traffic to the DNS server complex, 3) Deploy suitable Intrusion Prevention System in front of DNS servers, 4) Deploy additional DNS server capacity in a round-robin architecture, 5) Utilize DoS/DDoS tracking methods to identify the source(s) of the attack, or 6) Move name resolution service to a 3rd party provider.
7-7-8530	Recover from DHCP-based DoS Attack: If a DHCP (Dynamic Host Configuration Protocol) attack is underway, Network Operators and Service Providers should isolate the source to contain the attack. Plan to force all DHCP clients to renew leases in a controlled fashion at planned increments. Re-evaluate architecture to mitigate similar future incidents.
7-7-8531	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.

7-7-8532	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.
7-7-8533	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 thresholding 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 a traffic reroute.
7-7-8534	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.
7-7-8535	Recover from Voice over IP (VoIP) Device Masquerades or Voice over IP (VoIP) Server Compromise: If a Voice over IP (VoIP) server has been compromised, Network Operators and Service Providers should disconnect the server; the machine can be rebooted and reinitialized. Redundant servers can take over the network load and additional servers can be brought on-line if necessary. In the case of VoIP device masquerading, if the attack is causing limited harm, logging can be turned on and used for tracking down the offending device. Law enforcement can then be involved as appropriate. If VoIP device masquerading is causing significant harm, the portion of the network where the attack is originating can be isolated. Logging can then be used for tracking the offending device.
7-7-8540	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.
7-7-8548	Incident Response (IR) Procedures: When a service outage or security incident occurs, Network Operators and Service Providers should follow processes similar to Appendix X.
7-7-8549	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.
7-7-8551	Responding to New or Unrecognized Event: When responding to a new or unrecognized event, Network Operators and Service Providers should follow processes similar to Appendix Y.
7-7-8553	Sharing Information with Industry & Government during Recovery: During a security event, Network Operators, Service Providers and Equipment Suppliers should release to the National Communications Service National Coordination Center (ncs@ncs.gov) or US-CERT (cert@cert.org) information which may be of value in analyzing and responding to the issue, following review, edit and approval commensurate with corporate policy. Information is released

	<p>to these forums with an understanding redistribution is not permitted. Information which has been approved for public release and could benefit the broader affected community should be disseminated in the more popular security and networking forums such as NANOG and the SecurityFocus Mailing Lists.</p>
<p>7-7-8554</p>	<p>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. Example evidence handling processes are provided in Appendix X, Section 2f.</p>
<p>7-7-8555</p>	<p>Recovery from Lack of an Incident Communications Plan: If an incident occurs and a communications plan is not in place, Network Operators, Service Providers and Equipment Suppliers should, depending on availability of resources and severity of the incident, assemble a team as appropriate:</p> <ul style="list-style-type: none"> • In person • Conference Bridge • Other (Email, telephonic notification lists) <p>Involve appropriate organizational divisions (business and technical)</p> <ul style="list-style-type: none"> ◦ Notify Legal and PR for all but the most basic of events ◦ PR should be involved in all significant events ◦ Develop corporate message(s) for all significant events - disseminate as appropriate <p>If not already established, create contact and escalation procedures for all significant events.</p>
<p>7-7-8556</p>	<p>Recovery from the Absence of a Monitoring Requests Policy: In the absence of a monitoring request policy, Network Operators and Service Providers should refer all communications intercept requests to corporate counsel.</p>
<p>7-7-8557</p>	<p>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) understand 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.</p>
<p>7-7-8559</p>	<p>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).</p>
<p>7-7-8561</p>	<p>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</p>

	<p>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.</p>
<p>7-7-8562</p>	<p>Recovery from Denial of Service Attack - Unwitting Agent: If an infected (zombie) device is detected, Network Operators and Service Providers should isolate the box and check integrity of infrastructure and agent. Adjust firewall settings, patch all systems and restart equipment. Consider making system or hostile code available for analysis to 3rd party such as US-CERT, NCC, or upstream provider's security team if hostile code does not appear to be known to the security community. Review Incident Response Post-Mortem Checklist (NRIC BP 8548).</p>
<p>7-7-8565</p>	<p>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.</p>
<p>7-7-8566</p>	<p>Recovery from Unauthenticated Patching Systems. Network Operators, Service Providers and Equipment Suppliers should assure that patching distribution hosts properly sign all patches. Critical systems must only use OSs and applications which employ automated patching mechanisms, rejecting unsigned patches. If a patch fails or is considered bad, restore OS and applications from known good backup media.</p>
<p>7-7-8567</p>	<p>News Disinformation after Recovery: Network Operators, Service Providers and Equipment Suppliers should ensure that actions taken due to a spoofed, faked or distorted news item should be cross-correlated against other sources. Any actions taken should be 'backed out' and corrective measures taken to restore the previous state. News source authentication methods should be implemented to ensure future accuracy.</p>

SAVE AS EXCEL