NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
6-5-0500 (Deleted)	Recommend Deletion. Superseded by NRIC BP 8061		Deleted
6-5-0506 (Deleted)	Recommend Deletion Superseded by NRIC BP 8072, 8073, 8074, and 8075		Deleted
7-7-0507	**Attack Trace Back:** Service Providers, Network Operators 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).	See also NRIC BP 8074 & 8075 There are several techniques for trace back: "Practical Network Support for IP Trace back" by Stefan Savage et.al., Dept. of Computer Science and Engineering, Univ of Washington, Tech Report UW-CSE-2000-02-01 with a version published in the Proceedings of the 2000 ACM SIBCOMM pp256-306 Stockholm, Sweden, August 2000 Hash based as described in "Hash Based IP Traceback" by Alex C Snoeren et.al of BBN published in Proceedings of the 2001 ACM SIBCOMM, San Diego, CA August 2001 A physical network arrangement as described in "CENTERTRACK, An IP Overlay Network" by Robert Stone of UUNET presented at NANOG #17 October 5, 1999. John Ioannidis and Steven M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", NDSS, February 2002. http://www.ietf.org/rfc/rfc3882.txt	Changed
6-5-0523 (Deleted)	Recommend Deletion Superseded by NRIC BP 8000, 8008, 8015, 8051, and 8060		Deleted

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
6-5-0533 (Deleted)	Recommend Deletion Superseded by NRIC BP 8513, additional coverage in 8514, 8521, and 8092.		**Deleted**
'6-5-0537 (Deleted)	Recommend Deletion Superseded by NRIC BP 8062		**Deleted**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-0551	**SS7 Network Design:** Network Operators should design their SS7 network components and interfaces consistent with the base security guidelines of the NIIF Reference document Part 3, Appendix I. This document provides guidance for desirable security features for any network element (call agent, feature server, soft switch, cross connect, gateway, database) to reduce the risk of potentially service affecting security compromises of the signaling networks supporting the public telephone network. It identifies security functionality, which should be in place by design, device or procedure. It includes an assessment framework series of checklists.	www.atis.org/niif/index.asp Network Interconnection Interoperability Forum (NIIF) Reference Document NIIF 5001 The NIIF Interconnection Template (Network Interconnection Bilateral Agreement Template), Issue 3.0 ATIS0300004 See also NRIC BP 8052, 8053	Changed
6-5-0585 (Deleted)	Recommend Deletion Superseded by NRIC BP 8066		Deleted
6-6-0806 (Deleted)	Recommend Deletion Superseded by NRIC BP 8040-8045		Deleted
6-6-0807 (Deleted)	Recommend Deletion Superseded by NRIC BP 8040-8045		Deleted
6-6-0813 (Deleted)	Recommend Deletion Superseded by NRIC BP 8096		Deleted
6-6-5276 (Deleted)	Recommend Deletion Superseded by NRIC 8013.		Deleted

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-0808	**Release Filtering Information/Policies to Customers:**Service Providers and Network Operators should make information available to customers about traffic filtering (both static and dynamic), where required by law.	Economic Espionage Act 1996 Telecommunications Act 1996 Electronic Communications Privacy Act 1986 Graham-Leach-Bliley Act 2002 Sarbannes-Oxley 2003 USA PATRIOT Act 2002 Health Insurance Portability and Accountability Act (HIPAA) 2001 Supersedes 0809	**Changed**
6-6-0809 (Deleted)	Recommend Deletion Combined with NRIC BP 0808		**Deleted**
6-6-0811	Recommend removal of Cyber Security keyword. 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.		**Unchanged**
7-7-8000	**Disable Unnecessary Services:** Service Providers and Network Operators 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.	Configuration guides for security from NIST, US-CERT, NSA, SANS, vendors, etc. Related to NRIC BP 8502, 8505	**Changed**
7-7-8001	**Strong Encryption Algorithms and Keys:** Service Providers, Network Operators, and Equipment Suppliers should use industry-accepted algorithms and key lengths for all uses of encryption, such as 3DES or AES.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 Dependency on NRIC BP 8503	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
6-6-8002 (Deleted)	Recommend Deletion Superseded by NRIC BP 8004.		Deleted
7-7-8003	**Control Plane Reliability** Service Providers and Network Operators should minimize single points of failure 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.	Dependency on NRIC BP 8027, 8037	Changed
7-7-8004	**Harden Default Configurations:** Equipment Suppliers should work closely and regularly with US-CERT, NSA, and customers to provide recommendations concerning existing default settings and to identify future default settings which may introduce vulnerabilities. Equipment Suppliers should proactively collaborate with network operators to identify and provide recommendations on configurable default parameters and provide guidelines on system deployment and integration such that initial configurations are as secure as allowed by the technology.	Dependency on NRIC BP 8505. Supersedes NRIC BP 8002.	Changed
7-7-8005	**Document Single Points of Failure:** Service Providers and Network Operators should implement a continuous engineering process to identify and record single points of failure 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.	ISF SB52 Dependency on NRIC BP 8506	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8006	Protection of Externally Accessible Network Applications: Service Providers and Network Operators 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.	ISF CB63, NRIC BP 0510. Dependency on NRIC BP 8507, Related to NRIC BP 8111, 8112	Changed
7-7-8007	Define Security Architecture(s): Service Providers and Network Operators 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.	Octave Catalog of Practices, Version 2.0, CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice SP6.2; NIST Special Pub 800-12, NIST Special Pub 800-14 Dependency on NRIC BP 8508, 8005, 8117	Changed
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.	ISF SB52, http://www.sans.org Dependency on NRIC BP 8509, 8006	Changed
6-6-8009 (Deleted)	Recommend Deletion Superceded by BP 8134.		Deleted

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8010	**OAM&P Product Security Features:** Equipment Suppliers should implement current industry baseline requirements for Operations, Administration, Management, and Provisioning (OAM&P) security in products - software, network elements, and management systems.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	**Unchanged**
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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	**Unchanged**
7-6-8012	**Secure Communications for OAM&P Traffic:** To prevent unauthorized users from accessing Operations, Administration, Management, and Provisioning (OAM&P) systems, Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	**Unchanged**
7-6-8013	**Controls for Operations, Administration, Management, and Provisioning (OAM&P) Management Actions:** Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 . Supersedes NRIC BP 5276.	**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8014	OAM&P Privilege Levels: For OAM&P systems, Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 NRIC BP 0550	Unchanged
7-6-8015	Segmenting Management Domains: For OAM&P activities and operations centers, Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 NRIC BP 0547.	Unchanged
7-6-8016	OAM&P Security Architecture: Service Providers and Network Operators should design and deploy an Operations, Administration, Management, and Provisioning (OAM&P) security architecture based on industry recommendations.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 Also, NRIC BP 0510. Dependency on NRIC BP 8008	Unchanged
7-6-8017	OAM&P Protocols: Service Providers, Network Operators, 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	Unchanged

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8018	**Hardening OAM&P User Access Control:** Service Providers, Network Operators, 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	Changed
7-7-8019	**Hardening OSs for OAM&P:** Service Providers, Network Operators, and Equipment Suppliers with devices equipped with operating systems used for OAM&P should have operating system hardening procedures applied. Harding 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.	Configuration guides for security from NIST, US-CERT, NSA, SANS, vendors, http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 Dependency on NRIC BP 8004	Changed
7-7-8020	**Expedited Security Patching:** Service Providers, Network Operators, 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.	http://www.isaca-phoenix.org/2002to2003%20Presentations/January%2016,%202003%20-%20Next%20Attack.ppt). Related to NRIC BP 8035	Changed

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8021	**Switched Hubs for OAM&P Networks:** In critical networks for Operations, Administration, Management, and Provisioning (OAM&P), Service Providers, Network Operators, 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.		Unchanged
7-7-8022	**Remote Operations, Administration, Management and Provisioning (OAM&P) Access:** Service Providers and Network Operators 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	ISF CB53	Changed
7-6-8023	**Scanning Operations, Administration, Management and Provisioning (OAM&P) Infrastructure:** Service Providers and Network Operators 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.		Unchanged
7-7-8024	**Limited Console Access:** Service Providers, Network Operators, 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.	Some systems differentiate a local account database and network account database. Users should be authenticated onto the network using a network accounts database, not a local accounts database. http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003. Related to NRIC BP 8018 and 8113..	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8025	**Protection from SCADA Networks:** Telecom/Datacomm OAM&P networks for Service Providers and Network Operators should be isolated from other OAM&P networks, e.g., SCADA networks, such as for power, water, industrial plants, pipelines, etc. - 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."	Note: Service providers MAY provide an offer of 'managed' SCADA services or connectivity to other utilities. This should be separate from the provider's OAM&P network.	**Changed**
7-7-8026	**SNMP Vulnerability Mitigation:** Service Providers, Network Operators, and Equipment Suppliers should apply SNMP vulnerability patches to all systems on infrastructure networks because SNMP vulnerabilities can create significant risk.	Related to NRIC BP 8114, US-CERT	**Changed**
7-7-8027	**Source, Object, and Binary Code Integrity:** Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	**Changed**
7-6-8028	**Distribution of Encryption Keys:** When Service Providers, Network Operators, 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.		**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8029	Network Access to Critical Information: Service Providers, Network Operators, 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.		Unchanged
7-7-8030	OAM&P Session Times: For Service Providers, Network Operators, 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.		Changed
7-7-8031	LAES Interfaces and Processes: Service Providers, Network Operators, and Equipment Providers should develop and communicate Lawfully Authorized Electronic Surveillance (LAES) policy. They should: - 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	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 Also, NRIC BP 0505	Changed
7-6-8032	Patching Practices: Service Providers, Network Operators, and Equipment Suppliers should design and deploy a patching process based on industry recommendations, especially for critical OAM&P systems.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	Unchanged

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8033	**Software Development:** Service Providers, Network Operators, 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003. Also, NRIC BP 0535. Common Criteria: http://www.iso.org, http://csrc.nist.gov/cc/; Carnegie-Mellon Software Engineering Institute secure software development: http://www.sei.cmu.edu/engineering/engineering.html; Secure Programming Educational Material at http://www.cerias.purdue.edu/homes/pmeunier/secprog/sanitized/; http://www.atstake.com/services/smartrisk/application.html	**Changed**
7-7-8034	**Software Patching Policy:** Service Providers and Network Operators should define and incorporate a formal patch/fix policy into the organization's security policies.		**Changed**
7-6-8035	**Software Patch Testing:** The patch/fix policy and process used by Service Providers and Network Operators should include steps to appropriately test all patches/fixes in a test environment prior to distribution into the production environment.	Related to NRIC BP 8020.	**Unchanged**
7-6-8036	**Exceptions to Patching:** Service Provider and Network Operator 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.		**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8037	**System Inventory Maintenance:** Service Providers and Network Operators 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.	NRIC BP 0510.	**Unchanged**
7-6-8038	**Security Evaluation Process:** For Service Providers and Network Operators, 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.		**Unchanged**
7-6-8039	**Patch/Fix Verification:** Service Providers and Network Operators 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.		**Unchanged**
7-7-8040	**Mitigate Control Plane Protocol Vulnerabilities:** Service Providers and Network Operators 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.	See NRIC VI Cyber Security Focus group final report/recommendations Dependency on NRIC BP 8000, 8001, 8004, 8020 Related to NRIC BP 8115, 8116 Follow NRIC Best Practices for architectural and server hardening, and management controls to protect network elements and their management interfaces, especially elements with IP interfaces, against compromise and corruption. Supersedes NRIC BPs 0806 and 0807.	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8041	**Prevent Network Element Resource Saturation:** Equipment Suppliers for layer 3 switches/routers, with interfaces that mix user and control plane data, should provide filters and access lists on the header fields to protect the control plane from resource saturation by filtering out untrusted packets destined to for control plane. Measures may include: 1) Allowing the desired traffic type from the trusted sources to reach the control-data processor and discard the rest 2) separately rate-limiting each type of traffic that is allowed to reach the control-data processor, to protect the processor from resource saturation.	Dependency on NRIC BP 8523. Supersedes NRIC BPs 0806 and 0807.	**Unchanged**
7-7-8042	**BGP (Border Gateway Protocol) Validation:** Service Providers and Network Operators 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).	NSTAC ISP Working Group - BGP/DNS, Scalable key distribution mechanisms, NRIC V FG 4: Interoperability. Supersedes NRIC BPs 0806 and 0807.	**Changed**
7-6-8043	**Prevent BGP (Border Gateway Protocol) Poisoning:** Service Providers and Network Operators 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 un-authorized 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 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 7) Employ "Murphy filter" (guarded trust and mutual suspicion) to reinforce filtering your peer should have done.	http://www.cymru.com/Bogons/index.html, NSTAC ISP Working Group - BGP/DNS, RIPE-181, "A Route-Filtering Model for Improving Global Internet Routing Robustness" 222.iops.org/Documents/routing.html Dependency on NRIC BP 8525. Supersedes NRIC BPs 0806 and 0807.	**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8044	**BGP (Border Gateway Protocol) Interoperability Testing:** Service Providers and Network Operators 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.	NSTAC ISP Working Group - BGP/DNS, also NANOG (http://www.nanog.org) and MPLS Forum interoperability testing (http://www.mplsforum.org). Supersedes NRIC BPs 0806 and 0807.	**Unchanged**
7-6-8045	**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.	Dependency on NRIC BP 8526, http://www.ietf.org/rfc/rfc1321.txt Supersedes NRIC BPs 0806 and 0807.	**Unchanged**
7-7-8046	**Protect DNS (Domain Name System) Servers Against Compromise:** Service Providers and Network Operators 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.	RFC-2870 ISO/IED 15408 ISO 17799 US-CERT "Securing an Internet Name Server" Dependency on NRIC BP 8001, 8063, 8071, 8083, 8527. Related to NRIC BP 8117 and BP 8118.	**Changed**
7-6-8047	**Protect Against DNS (Domain Name System) Denial of Service:** Service Providers and Network Operators 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.	RFC-2870, ISO/IEC 15408, ISO 17799, US-CERT "Securing an Internet Name Server" (http://www.cert.org/archive/pdf/dns.pdf) Dependency on NRIC BP 8074, 8528. Related to NRIC BP 8118	**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8048	**Protect DNS (Domain Name System) from Poisoning:** Service Providers, Network Operators, 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.	RFC-1034, RFC-1035, RFC-2065, RFC-2181, RFC-2535, ISC BIND 9.2.1 US-CERT "Securing an Internet Name Server" (http://www.cert.org/archive/pdf/dns.pdf) Dependency on NRIC BP 8527.	**Unchanged**
7-6-8049	**Protect DHCP (Dynamic Host Configuration Protocol) Server from Poisoning:** Service Providers and Network Operators 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.	draft-ietf-dhc-csr-07.txt, RFC 3397, RFC2132, RFC1536, RFC3118. Dependency on NRIC BP 8001, 8530.	**Unchanged**
7-6-8050	**MPLS (Multi-Protocol Label Switching) Configuration Security:** Service Providers and Network Operators 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.	IETF RFC 2547, RFC 3813 & draft-ietf-l3vpn-security-framework-02.txt Dependency on NRIC BP 8531.	**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8051	**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 confidentialit mechanisms (e.g., digital signature and encrypted VPN tunneling).	NRIC BP 0547, ITU SS7 Standards, “Securing SS7 Telecommunications Networks”, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 5-6 June 2001.	Unchanged

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8052	**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.	NRIC BP 0551. Also, NIIF Guidelines for SS7 Security. Dependency on NRIC BP 8532.	**Unchanged**
7-6-8053	**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.	NRIC BP 0551. Dependency on NRIC BP 8533.	**Unchanged**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8054	**Anonymous Use of SS7 Services or Services Controlled by SS7:** Network Operators should have defined policies and process for addition and configuration of SS7 elements to the various tables. Process should include the following: personal verification of the request (e.g., one should not simply go forward on a faxed or emailed request without verifying that it was submitted legitimately), approval process for additions and changes to SS7 configuration tables (screening tables, call tables, trusted hosts, calling card tables, etc.) to ensure unauthorized elements are not introduced into the network. Companies should also avoid global, non-specific rules that would allow unauthorized elements to connect to the network. Screening rules should be provisioned with the greatest practical depth and finest practical granularity in order to minimize the possibility of receiving inappropriate messages. Network operators should log translation changes made to network elements and record the user login associated with each change. These practices do not mitigate against the second threat mentioned below, the insertion of inappropriate data within otherwise legitimate signaling messages. To do so requires the development of new capabilities, not available in today's network elements.	NRIC BP 0551. Dependency on NRIC BP 8534.	**Unchanged**
7-6-8055	**Voice over IP (VoIP) Device Masquerades:** Network Operators and Equipment Suppliers supplied VoIP CPE devices need to support authentication service and integrity services as standards based solutions become available. Network Operators need to turn-on and use these services in their architectures.	PacketCable Security specifications. Dependency on NRIC BP 8536.	**Unchanged**
7-7-8056	**Operational Voice over IP (VoIP) Server Hardening:** Network Operators should ensure that network servers have authentication, integrity, and authorization to prevent inappropriate use of the servers. Enable logging to detect inappropriate use.	PacketCable Security specifications. Dependency on NRIC BP 8001, 8536.	**Changed**
7-6-8057	**Voice over IP (VoIP) Server Product Hardening:** Equipment Suppliers should provide authentication, integrity, and authorization mechanisms to prevent inappropriate use of the network servers. These capabilities must apply to all levels of user -- users, control, and management.	PacketCable Security specifications. Dependency on NRIC BP 8001 related to NRIC BP 8049.	**Unchanged**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8058	**Protect Cellular Service from Anonymous Use:** Service Providers and Network Operators 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.	Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc. Dependency on NRIC BP 8001, 8537. Related to NRIC BP 8106.	Unchanged
7-6-8059	**Protect Cellular Data Channel:** Service Providers and Network Operators 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).	Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc.	Unchanged
7-6-8060	**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.	Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc. Dependency on NRIC BP 8001, 8020, 8537.	Unchanged
7-6-8061	**IR (Incident Response) Procedures:** Service Providers and Network Operators should establish a set of standards and procedures for dealing with computer 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.	IETF RFC2350, US-CERT. Also, NRIC BP 8074, and 8075, 0561, 0598, 0599. Supersedes NRIC BP 0500.	Unchanged

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8062	**IR (Incident Response) Team:** Service Providers and Network Operators 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.	IETF RFC2350, CMU/SEI-98-HB-001. Also, NRIC BP 0598. Supersedes NRIC BP 0537.	**Changed**
7-7-8063	**Intrusion Detection/Prevention Tools (IDS/IPS):** Service Providers and Network Operators should install and actively monitor IDS/IPS tools. Sensor placement should focus on resources critical to the delivery of service.	NRIC BP 8072, 8073, 8074, 8075, and 0608.	**Changed**
7-7-8064	**Security-Related Data Collection**Service Providers and Network Operators 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).	Related to NRIC BP 8119, BP 8139, and BP 0518.	**Changed**
7-7-8065	**Sharing Information with Law Enforcement:** Service Providers, Network Operators, 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.	NRIC BP 0561.	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8066	**Sharing Information with Industry & Government:** Service Providers, Network Operators, and Equipment Suppliers should participate in regional and national information sharing groups such as the National Coordinating Center for Telecommunications (NCC), Telecom-ISAC, and the ISP-ISAC (when chartered). 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.	Related to NRIC BP 8553. Supersedes NRIC BP 0585.	**Unchanged**
7-7-8067	**Evidence Collection Guidelines:** Service Providers and Network Operators 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.	IETF RFC3227, http://www.cybercrime.gov	**Changed**
7-7-8068	**Incident Response Communications Plan:** Service Providers, Network Operators, 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.	NRIC BP 0561, 0598, 0609. Also related to NRIC BP 8066 and 8555.	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-6-8069	**Monitoring Requests:** Service Providers, Network Operators, 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.	Dependency on NRIC BP 8031.	**Unchanged**
7-7-8070	**Abuse Reporting:** Service Providers and Network Operators 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.”	Related to NRIC BP 8513 and 8092. Supersedes NRIC BP 0533.	**Changed**
7-6-8071	**Threat Awareness:** Service Providers and Network Operators 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.	Dependency on NRIC BP 8034 and 8035.	**Unchanged**
7-7-8072	**Intrusion Detection/Prevention Tools (IDS/IPS) Maintenance:** Service Provider and Network Operator should maintain and update IDS/IPS tools regularly to detect current threats, exploits, and vulnerabilities.	Related to 8020. Supersedes NRIC BP 0506.	**Changed**
7-7-8073	**Intrusion Detection/Prevention (IDS/IPS) Tools Deployment:** Service Providers and Network Operators 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.	Supersedes NRIC BP 0506.	**Changed**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8074	**Denial of Service (DoS) Attack - Target:** Where possible, Service Provider and Network Operator networks and Equipment Supplier 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.	Related to NRIC BP 8561. Supersedes NRIC BP 0506.	Changed
7-7-8075	**Denial of Service (DoS) Attack - Agent (Zombies):** Service Provider and Network Operator should periodically scan hosts for signs of compromise. Where possible, monitor bandwidth utilization and traffic patterns for signs of anomalous behavior.	Related to NRIC BP 8562. Supersedes NRIC BP 0506.	Changed
7-7-8076	**Denial of Service (DoS) Attack - Vendor:** Equipment Suppliers should develop effective DoS/DDoS survivability features for their product lines.	e.g., SYN Flood attack defense, CERT/CC® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - http://www.cert.org/advisories/CA-1996-21.html. Related to NRIC BP 8563.	Changed

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8077	Compensating Control for Weak Authentication Methods: For Service Provider and Network Operator 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.	 In the long term, the vendor should be engaged to correct the issue, either by allowing the built in method to be changed periodically, or by allowing the user to add complementary authentication means that they control, hence creating a two-factor authentication. Where authentication methods must be shared, create an enforceable authentication method policy that addresses the periodic changing of the characteristics of the authentication method, and the dissemination of the method based on the principle of least privilege. If the authentication methods are shared, policy to implement least privilege access and periodic authentication characteristic change should be developed and implemented. Consider replacement of device at end of life, especially if the device is protecting key equipment. Implement a periodic audit program to verify policy compliance. Garfinkel, Simson, and Gene Spafford. “Users and Passwords”. Practical Unix & Internet Security, 2nd ed. Sebastopol, CA: O’Reilly and Associates, Inc. 1996. 49-69 King, Christopher M., Curtis E. Dalton, and T. Ertem Os	Changed
7-6-8078	Protect User IDs and Passwords During Network Transmission: Service Provider, Network Operators, and Equipment Suppliers should not send user IDs and passwords in the clear, or send passwords and user IDs in the same message/packet.	US Government and National Security Telecommunications Advisory Committee (NSTAC) ISP Network Operations Working Group. “Short Term Recommendations”. Report of the ISP Working Group for Network Operations/Administration. May 1, 2002.	Unchanged

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8079	**Use Strong Passwords:** Service Provider, Network Operators, 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.	Garfinkel, Simson, and Gene Spafford. "Users and Passwords". Practical Unix & Internet Security, 2nd ed. Sebastopol, CA: O'Reilly and Associates, Inc. 1996. 49-69 US Government and National Security Telecommunications Advisory Committee (NSTAC) ISP Network Operations Working Group. "Short Term Recommendations". Report of the ISP Working Group for Network Operations/Administration. May 1, 2002. http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003.	**Changed**
7-7-8080	**Change Passwords on a Periodic Basis:** Service Providers, Network Operators, 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.	Garfinkel, Simson, and Gene Spafford. "Users and Passwords". Practical Unix & Internet Security, 2nd ed. Sebastopol, CA: O'Reilly and Associates, Inc. 1996. 49-69 US Government and National Security Telecommunications Advisory Committee (NSTAC) ISP Network Operations Working Group. "Short Term Recommendations". Report of the ISP Working Group for Network Operations/Administration. May 1, 2002. http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003	**Changed**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8081	**Protect Authentication Methods:** Service Providers, Network Operators, 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.	Garfinkel, Simson, and Gene Spafford. “Users and Passwords”. Practical Unix & Internet Security, 2nd ed. Sebastopol, CA: O’Reilly and Associates, Inc. 1996. 49-69 US Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE). “Administration of Static Passwords and User Ids”. Operations, Administration, Maintenance, & Provisioning (OAM&P) Security Requirements for Public Telecommunications Network. Draft 2.0, August 2002. http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003. This best practice should be reinforced with best practices related to awareness, education, audits, and violation handling as provided in NRIC BPs 8121 through 8125. Supersedes NRIC BP 8082.	Changed
'6-6-8082 (Deleted)	Recommend Deletion Superceded by BP 8081.	King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. “Security Infrastructure Design Principles”. Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 111-140 Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Digital Signatures and Certification Authorities - Technology, Policy, and Legal Issues". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 263-294 McClure, Stuart, Joel Scambray, George Kurtz. "Dial-Up, PBX, Voicemail, and VPN Hacking". Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition. Berkley, CA. The McGraw-Hill Companies. 2001. 393-440.	Deleted

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8083	Protect Authentication Files and/or Databases: Authentication databases/files used by Service Providers, Network Operators, 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.	Garfinkel, Simson, and Gene Spafford. “Users, Groups, and the Superuser”. Practical Unix & Internet Security, 2nd ed. Sebastopol, CA: O’Reilly and Associates, Inc. 1996. 71-137 King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. “Platform Hardening”. Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 256-284 National Institute of Standards and Technology. “Secure Authentication Data as it is Entered”. Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996 McClure, Stuart, Joel Scambray, George Kurtz. "Enumeration". Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition. Berkley, CA. The McGraw-Hill Companies. 2001. 63-112.	Changed
7-7-8084	Create Trusted PKI Infrastructure When Using Generally Available PKI Solutions: When using digital certificates, Service Providers, Network Operators, 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.	Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Digital Signatures and Certification Authorities - Technology, Policy, and Legal Issues". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 263-294.	Changed
7-7-8085	Expiration of Digital Certificates: For Service Providers, Network Operators, 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.	McClure, Stuart, Joel Scambray, George Kurtz. "Dial-Up, PBX, Voicemail, and VPN Hacking". Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition. Berkley, CA. The McGraw-Hill Companies. 2001. 393-440. Related to NRIC BP 8120.	Changed

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8086	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), Service Providers and Network Operators should develop processes to determine which users require access to a specific device or application. Equipment Suppliers should provide capability to support access levels.	These processes should be used to develop criteria for determining who can be authorized to access a specific device or application. The criteria can be used to develop and implement access privilege levels (for example, role-based access, tiered access) for specific devices or applications. These levels may provide authorization for certain users to perform specific functions. Garfinkel, Simson, and Gene Spafford. “Personnel Security”. Practical Unix & Internet Security, 2nd ed. Sebastopol, CA: O’Reilly and Associates, Inc. 1996. 389-395 King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. “Applying Policies to Derive the Requirements”. Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 66-110 National Institute of Standards and Technology. “Access Control Mechanisms, Access Control Lists (ACLs)”. Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996 Information Security Forum. “Access Control Policies”. The Forum’s Standard of Good Practice, The Standard for Inform	Changed
7-6-8087	Use Time-Specific Access Restrictions: Service Providers and Network Operators 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.	Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Access Controls - Two Views". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 242-261. Related to NRIC BP 8119.	Unchanged
7-7-8088	Develop Regular Access Audit Procedures: Service Providers, Network Operators, 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.	This best practice should be reinforced with best practices related to auditing as provided in NRIC BPs 8127 and BP 8128. Information Security Forum. “Security Audit/Review”. The Forum’s Standard of Good Practice, The Standard for Information Security. November 2000.	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8089	**Conduct Risk Assessments to Determine Appropriate Security Controls:** Service Providers, Network Operators, 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.	Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Access Controls - Two Views". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 242-261	Changed
7-6-8090	**Restrict Use of Dynamic Port Allocation Protocols:** Service Providers, Network Operators, 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.		Unchanged
7-7-8091	**Protect Cached Security Material:** Service Providers, Network Operators, 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.		Changed
7-7-8092	**Adopt and Enforce Acceptable Use Policy:** Service Providers and Network Operators should adopt a customer-directed policy whereby misuse of the network would lead to measured enforcement actions up to and including termination of services.	IETF rfc3013 section 3 and NANOG ISP Resources (http://www.nanog.org/isp.html). Also, NRIC BP 5145 and 8070. Supersedes NRIC BP 0533.	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
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).	IETF rfc3013 sections 4.3 and 4.4 and NANOF ISP Resources. www.IATF.net	**Unchanged**
7-6-8094	**Strong Encryption for Customer Clients:** Service Providers should implement customer client software that uses the strongest permissible encryption appropriate to the asset being protected.	http://www.securityforum.org and http://www.sans.org/resources/; Schneier, Bruce. 1996. Applied Cryptography. 2d.ed. John Wiley & Sons. See also NRIC BP 5162.	**Unchanged**
7-7-8095	**Establish System Resource Quotas:** Service Providers and Network Operators should establish, 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.		**Changed**
7-6-8096	**Users Should Employ Protective Measures:** Service Providers and Network Operators 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.	http://www.stonybrook.edu/nyssecure, http://www.fedcirc.gov/homeusers/HomeComputerSecurity/ Industry standard tools (e.g., LC4). See also NRIC BP 5165, BP 8134, BP 8135. Supersedes NRIC BP 0813.	**Unchanged**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8097	**Create Policy on Information Dissemination:** Service Providers, Network Operators, 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.	Octave Catalog of Practices, Version 2.0,CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice OP3.1.1& OP3.2.1; NIST Special Pub 800-12. King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. “Validation and Maturity”. Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 443-470 McClure, Stuart, Joel Scambray, George Kurtz. "Advanced Techniques". Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition. Berkley, CA. The McGraw-Hill Companies. 2001. 553-590 Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Risk Management and Architecture of Information Security (INFOSEC)". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 69-90. See also NRIC BPs: 5019, 5024, 5067, 5109 and 5285.	**Changed**
7-7-8098	**Create Policy on Removal of Access Privileges:** Service Providers, Network Operators, 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.	Octave Catalog of Practices, Version 2.0,CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice OP1.3.1-OP1.3.2, OP3.2.1-OP3.3 and OP3.1.1-Op3.1.3; NIST Special Pub 800-26; OMB Circular A-130 Appendix III. US Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE). “Administration of Static Passwords and User Ids”. Operations, Administration, Maintenance, & Provisioning (OAM&P) Security Requirements for Public Telecommunications Network. Draft 2.0, August 2002. See NRIC VI BPs 5015 and 5016. See also NRIC BP 8554.	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8099	**Create Policy on Personnel Hiring Merits:** Service Providers, Network Operators, 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.	See NRIC BP 8554. See also NRIC BPs 5033, 5034, 5065, and 8519.	**Changed**
7-7-8100	**Training for Security Staff:** Service Providers, Network Operators, 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.	Octave Catalog of Practices, Version 2.0,CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice SP1.2 & SP1.3. See also NRIC BP 5096, 8129, and 8130.	**Changed**
7-6-8101	**Document and Verify All Security Operational Procedures:** Service Providers and Network Operators 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.	Octave Catalog of Practices, Version 2.0,CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice SP1.2 & SP1.3. ISO 17799. See also NRIC VI BPs 5025 and 5067.	**Unchanged**
7-6-8102	**Discourage Use of Personal Equipment for Corporate Activities:** Service Providers, Network Operators, and Equipment Suppliers should discourage the use of personal equipment for telecommuting, virtual office, remote administration, etc.		**Unchanged**
7-7-8103	**Protect Network/Management Infrastructure from Malware:** Service Providers and Network Operators should deploy malware protection tools where feasible, establish processes to keep signatures current, and establish procedures for reacting to an infection.	www.cert.org/security-improvement/practices/p072.html, www.cert.org/security-improvement/practices/p096.html Dependency on NRIC BP 8548 and BP 8136 Note: Service providers may choose to offer virus protection as a value-added service to their customers as part of a service offering, but that is not required by this Best Practice.	**Changed**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8104	Proper Wireless LAN/MAN Configurations: Service Providers and Network Operators 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.		Changed
7-7-8105	Protection of Cellular User Voice Traffic: Service Providers and Network Operators 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).	Cellular Standards: GSM, GPRS, PCS2000, CDMA, 1XRTT, UMTS, 3GPP, 3GPP2	Changed
7-7-8106	Protect 3G Cellular from Cyber Security Vulnerabilities: Service Providers, Network Operator, 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.	IPSec. Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc. Dependency on NRIC BP 5018.	Changed
7-7-8108	Authentication System Failure: In the event of an authentication system failure, Service Providers and Network Operators 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> 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 t	Related to NRIC BP 8566.	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8109	**Automated Patch Distribution Systems:** Service Providers, Network Operators, 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.		**Changed**
7-7-8110	**News Disinformation:** Information from news sources may be spoofed, faked, or manipulated by potential attackers. Service Providers, Network Operators, and Equipment Suppliers should ensure news sources are authenticated and cross-verified to ensure accuracy of information, especially when not from a trusted source.	Related to NRIC BP 8517	**Changed**
7-7-8111	**Protect Sensitive Data in Transit for Externally Accessible Applications:** Service Providers and Network Operators 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.	Related to NRIC BP 8006, 8112	**New**
7-7-8112	**Protect Management of Externally Accessible Systems:** Service Providers and Network Operators 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.	Related to NRIC BP 8006, 8111	**New**
7-7-8113	**Limited Local Logon:** Service Providers, Network Operators, 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.	Some systems differentiate a local account database and network account database. Users should be authenticated onto the network using a network accounts database, not a local accounts database. http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003. Related to NRIC BP 8024	**New**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
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.	Related NRIC BP 8026	New
7-7-8115	**Mitigate Control Plane Protocol Vulnerabilities in Suppliers Equipment** 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	Related to NRIC BP 8040 See NRIC VI Cyber Security Focus group final report/recommendations Dependency on NRIC BP 8000, 8001, 8004, 8020	New
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.	ATIS Packet Technologies and Systems Committee (previously part of T1S1) ATIS Protocol Interworking Committee (previously part of T1S1) Related to NRIC BP 8040 See NRIC VI Cyber Security Focus group final report/recommendations Dependency on NRIC BP 8000, 8001, 8004, 8020	New
7-7-8117	**DNS Servers Disaster Recovery Plan:** Service Providers and Network Operators should prepare a disaster recovery plan to implement upon DNS server compromise.	Related NRIC BP 8046	New
7-7-8118	**Protect Against DNS (Domain Name System) Distributed Denial of Service:** Service Providers and Network Operators 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.	RFC-2870, ISO/IEC 15408, ISO 17799,US-CERT "Securing an Internet Name Server" (http://www.cert.org/archive/pdf/dns.pdf) Dependency on NRIC BP 8074, 8528. Related to NRIC BP 8047	New
7-7-8119	**Security-Related Data Correlation**Service Providers and Network Operators 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.	Related to NRIC BP 8064	New

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8120	**Revocation of Digital Certificates** Service Providers, Network Operators, and Equipment Suppliers should use equipment and products that support a central revocation list and revoke certificates that are suspected of having been compromised.	Related to NRIC BP 8085	New
7-7-8121	**Conduct Regular Audits of Information Security Practices:** Service Providers, Network Operators, and Equipment Providers should conduct regular audits of their Information Security practices.	ISO17799: http://www.iso.org COBIT: http://www.isaca.org OCTAVE: http://www.cert.org/octave/	New
7-7-8123	**Handle Policy Violations Consistently:** Service Providers, Network Operators, 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.		New
7-7-8124	**Conduct Organization Wide Security Awareness Training:** Service Providers, Network Operators, 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.	NIST: www.nist.gov Document is SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003 Related to NRIC BP 8033, BP 8100, BP 8129.	New
7-7-8125	**Policy Acknowledgement:** Service Providers, Network Operators, and Equipment Suppliers should ensure that employees formally acknowledge their obligation to comply with their corporate Information Security policies.		New

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8126	**Use Risk-Appropriate Authentication Methods:** Service Providers, Network Operators, 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).	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003.	**New**
7-7-8127	**Verify Audit Results Through Spot-Checking** Service Providers, Network Operators, and Equipment Suppliers should validate any regular auditing activity through spot-checking to validate the competency, thoroughness, and credibility of those regular audits.	Related to NRIC BP 8088	**New**
7-7-8128	**Promptly Address Audit Findings:**Service Providers, Network Operators, 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.	Related to NRIC BP 8088	**New**
7-7-8129	**Staff Training on Technical Products and Their Controls:** To remain current with the various security controls employed by different technologies, Service Providers, Network Operators, and Equipment Suppliers should ensure that technical staff participate in ongoing training and remain up-to-date on their certifications for those technologies.	Related to NRIC BP 8100.	**New**
7-7-8130	**Staff Trained on Incident Reporting:**Service Providers, Network Operators, and Equipment Suppliers should provide procedures and training to staff on the reporting of security incidents, weaknesses, and suspicious events.	Related to NRIC BP 8100.	**New**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8131	**Include Security Incidents in Business Recovery Plan: A** Service Provider's or Network Operator's Business Recovery Plan should factor in potential Information Security threats of a plausible likelihood or significant business impact.		**New**
7-7-8132	**Leverage Business Impact Analysis for Incident Response Planning:**Service Providers and Network Operators should leverage the BCP/DR Business Impact Assessment (BIA) efforts as input to prioritizing and planning Information Security Incident Response efforts.	Related to NRIC BPs 8061, 1003, and 1005.	**New**
7-7-8133	**Consistent Security Controls for DR Configurations:**A Service Provider's or Network Operator's disaster recovery or business continuity solutions should adhere to the same Information Security best practices as the solutions used under normal operating conditions.	Related to NRIC BPs 1003 and 1005.	**New**
7-7-8134	**Security of Devices Beyond Scope of Control** Service Providers should carefully consider possible impacts on their networks from changes in the configuration or authentication information on devices beyond the service demarcation point, and thus beyond their physical or logical scope of control. Service Providers should consider network filters or network authentication to protect against malicious traffic or theft of service caused by such insecure devices.	www.tialonline.org/standars/sfg/tr-41 Related to NRIC BP 8135	**New**
7-7-8135	**Protection of Devices Beyond Scope of Control** Equipment Suppliers should implement techniques such as tamper-proof crypto-chips/authentication credentials and authentication for (service provider) configuration controls, in customer premises equipment.	PacketCableTM Security Specification PKT-SP-SEC-I11-040730, IETF RFC 3261, Related to BP 8134	**New**
7-7-8136	**Protect Network/Management Infrastructure from Unexpected File System Changes:** Service Providers and Network Operators 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.	www.cert.org/security-improvement/practices/p072.html, www.cert.org/security-improvement/practices/p096.html Dependency on NRIC BP 8548. Related to BP 8103.	**New**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8137	**Notification Diversity** Equipment Suppliers (hardware and software) should support diverse notification methods, such as using both e-mail, websites, and tech support in order to properly notify users of newly discovered relevant vulnerabilities, viruses, or other threats.	This could mitigate , for example, the communication blockage that could be caused when a virus blocks e-mail distribution channels.	New
7-7-8138	**Renewal of Digital Certificates** Service Providers, Network Operators, 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.	Related to NRIC BP 8085, 8120	New
7-7-8139	**Security-Related Data Analysis:**Service Providers and Network Operators 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.	Related to NRIC BP 8064	New
7-7-8500	**Recovery from Digital Certificate Key Compromise:** In the event the key in a digital certificate becomes compromised, Service Providers, Network Operators, 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.	Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Digital Signatures and Certification Authorities - Technology, Policy, and Legal Issues". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 263-294. Nash, Andrew, William Duane, Celia Joseph, Derek Brink. "Key and Certificate Life Cycles". PKI Implementing and Managing E-Security. Berkley CA. The McGraw-Hill Companies. 2001. 139-178. NRIC BP 8548 & 8551	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8501	**Recovery from Root Key Compromise:** In the event the root key in a digital certificate becomes compromised, Service Providers, Network Operators, and Equipment Providers 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.	Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Digital Signatures and Certification Authorities - Technology, Policy, and Legal Issues". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 263-294. Nash, Andrew, William Duane, Celia Joseph, Derek Brink. "Key and Certificate Life Cycles". PKI Implementing and Managing E-Security. Berkley CA. The McGraw-Hill Companies. 2001. 139-178. NRIC BP 8548 & 8551	**Changed**
7-7-8502	**Recovery from Vulnerable or Unnecessary Services:** When a compromise occurs, or new exploits are discovered, Service Providers and Network Operators 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.	Configuration guides for security from NIST, US-CERT, NSA, SANS, vendors, etc. Related to NRIC BP 8000	**Changed**
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, Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 802.11i & 802.16 Related to NRIC BP 8001	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
6-6-8504 (Deleted)	Recommend Deletion Superseded by NRIC BP 8506.		Deleted
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, Service Providers and Network Operators 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.	Related to NRIC BP 8004	Changed
7-7-8506	**Document Single Points of Failure During Recovery:** Following a compromise and reestablishment of lost service, Service Providers and Network Operators should re-evaluate the architecture for single points of failure. 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.	ISF SB52, Related to NRIC BP 8006. Supersedes NRIC BP 8504.	Changed
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, Service Providers and Network Operators 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.	http://www.atis.org/ - T1 276-2003 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: July, 2003 ISF CB63, NRIC BP 0510, 8006, 8011, 8012	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8508	Post-Mortem Review of Security Architecture after Recovery: Immediately following incident recovery, Service Providers and Network Operators 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.	Octave Catalog of Practices, Version 2.0,CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice SP6.2; NIST Special Pub 800-12, NIST Special Pub 800-14, Related to NRIC BP 8007	Changed
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, Service Providers and Network Operators should, as part of a post-mortem process, review segmentation design to evaluate adequacy of the architecture and data isolation.	ISF SB52, www.sans.org, Related to NRIC BP 8008	Changed
7-7-8510	Recover from Compromise of Sensitive Information Stored on Network Systems/Elements: When compromise or trust violations occur, Service Providers, Network Operators and Equipment Providers 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.	FIPS 140-2, PUB 46-3, PUB 74, PUB 81, PUB 171, PUB 180-1, PUB 197, ANSI X9.9, X9.52, X9.17	Changed
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, Service Providers and Network Operators 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.	IETF rfc3013 section 3 and NANOG ISP Resources (www.nanog.org/isp.html) See also NRIC BP 5145, 8070, 8092	Changed
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.	IETF rfc3013 sections 4.3 and 4.4. NANOG ISP Resources. www.IATF.net. Related NRIC BP 8093, 8073	Changed
7-7-8515	Recovery from Misuse or Undue Consumption of System Resources: If a misuse or unauthorized use of a system is detected, Service Providers and Network Operators should perform forensic analysis on the system , conduct a post-mortem analysis and establish system resource quotas.	Dependency on NRIC BP 8095, 8548, 8554, 8564	Changed

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8517	Recovery from Unauthorized Information Dissemination: If information has been leaked or the release policy has not been followed, Service Providers, Network Operators, 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.	Octave Catalog of Practices, Version 2.0,CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice OP3.1.1& OP3.2.1; NIST Special Pub 800-12. King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. “Validation and Maturity”. Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 443-470 McClure, Stuart, Joel Scambray, George Kurtz. "Advanced Techniques". Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition. Berkley, CA. The McGraw-Hill Companies. 2001. 553-590 Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Risk Management and Architecture of Information Security (INFOSEC)". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 69-90. See also the following NRIC BPs: 5019, 5024, 5067, 5109, and 8110.	Changed
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, Service Providers, Network Operators, and Equipment Suppliers should undertake one or more of the following: 1) Provide additional employee training. 2) Reassign, dismiss, or discipline the employee.	See NRIC BP 8554, 8099, 5033, 5034 and 5065.	Changed
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), Service Providers and Network Operators 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.		Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8522	Recover from Discovery of Unsanctioned Devices on the Organizational Network: Upon discovery of an unsanctioned device on the organizational network, Service Providers, and Network Operators 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. Conduct review of policies to determine: 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? If the use is deemed malicious/suspect, coordinate with legal counsel: 1. Based on counsel's advice, consider collecting additional data for the purposes of assessing 2. Depending on the scope of the misuse, consider a referral to law enforcement. 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. 3.a. Depending on severity of the issue, arrange for permanent/temporary suspension of syste 3.b. Confront user regarding personnel/HR policies. Ensure user does not have access to netv 3.c. Disconnect system from network before allowing user access. 3.d. Request permission to examine system (see evidence/forensic procedures section if permi 3.e. If permission to review system is denied, follow-up with Legal/HR about the disposition of t 3.f. Follow HR procedures regarding disciplinary actions. 4. Conduct review of policies to determine: 4.a. If additional staff education regarding acceptable use of network/computing resources is re 4.b. If security monitoring and awareness procedures adequately protect organization.	Related NRIC BP 8012	Changed
7-7-8523	Recovery from Network Element Resource Saturation Attack: If the control plane is under attack, Service Providers and Network Operators 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.		Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8525	**Recovery from BGP (Border Gateway Protocol) Poisoning:** If the routing table is under attack from malicious BGP updates, Service Providers and Network Operators 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.	RIPE-181, "A Route-Filtering Model for Improving Global Internet Routing Robustness" www.iops.org/Documents/routing.html Related to NRIC BP 8042	**Changed**
7-7-8526	**Recover from Interior Routing Table Corruption:** If the interior routing has been corrupted, Service Providers and Network Operators 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.		**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, Service Providers and Network Operators 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.	RFC-2870, ISO/IEC, 15408, ISO 17799, US-CERT "Securing an Internet Name Server" Dependency on NRIC BP 8046, 8117, 8063, 8071, 8083	**Changed**
7-7-8528	**Recover from DNS (Domain Name Server) Denial of Service Attack:** If the DNS server is under attack, Service Providers and Network Operators 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.	RFC-2870, ISO/IEC 15408, ISO 17799 US-CERT "Securing an Internet Name Server" Dependency on NRIC BP 8046, 8117, 8063, 8071	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8530	**Recover from DHCP-based DoS Attack:** If a DHCP ((Dynamic Host Configuration Protocol) attack is underway, Service Provider and Network Operators 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.	PacketCable Security specification, NRIC BP 8049	**Changed**
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, Service Provider and Network Operators 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.	IETF RFC 2547, 8050	**Changed**
7-7-8532	**Recover from SCP Compromise:** No prescribed standard procedures exist for Service Providers and Network Operators 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.	NRIC BP 0551	**Changed**
7-7-8533	**Recover from SS7 DoS Attack:** If an SS7 Denial of Service (DoS) attack is detected, Service Provider and Network Operators 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.	NRIC BP 0551, 8053	**Changed**
7-7-8534	**Recover from Anonymous SS7 Use:** If logs or alarms determine an SS7 table has been modified without proper authorization, Service Provider and Network Operators 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.	NRIC BP 0551, 8052	**Changed**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
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, Service Provider and Network Operators 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.	PacketCable Security specification, NRIC BP 8055	**Changed**
7-7-8537	**Recover from Cellular Service Anonymous Use or Theft of Service:** If anonymous use or theft of service is discovered, Service Providers and Network Operators 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.	Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc. Dependency on NRIC BP 8001, 8058	**Changed**
7-7-8539	**Recover from Cellular Network Denial of Service Attack:** If the attack is IP based, Service Provider and Network Operators 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).	Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc. Dependency on NRIC BP 5018, 8060	**Changed**
7-7-8540	**Recover from Unauthorized Remote OAM&P Access:** When an unauthorized remote access to an OAM&P system occurs, Service Providers and Network Operators 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.	ISF CB53, NRIC BP 8046	**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8548	**Incident Response (IR) Procedures:** When a service outage or security incident occurs, Service Providers and Network Operators should follow processes similar to Appendix X.	IETF RFC2350, US-CERT NRIC BP 8074, 8075, 0561, 0598, 0599	**Changed**
7-7-8549	**Lack of Business Recovery Plan:** When a Business Recovery Plan (BRP) does not exist, Service Providers and Network Operators 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.	IETF RFC2350, CMU/SEI-98-HB-001 NRIC BP 0598, 8548	**Changed**
7-7-8551	**Responding to New or Unrecognized Event:** When responding to a new or unrecognized event, Service Providers and Network Operators should follow processes similar to Appendix Y.	NRIC BP 0518	**Changed**
7-7-8553	**Sharing Information with Industry & Government during Recovery:** During a security event, Service Providers, Network Operators, 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 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.	NRIC BP 8066	**Changed**

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8554	**Evidence Collection Procedures during Recovery:** Insomuch as is possible without disrupting operational recovery, Service Providers and Network Operators 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.	IETF RFC3227, www.cybercrime.gov 8548	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8555	**Recovery from Lack of an Incident Communications Plan:** If and incident occurs and a communications plan is not in place, Service Providers, Network Operators, and Equipment Suppliers should , depending on availability of resources and severity of the incident, assemble a team as appropriate: - In person - Conference Bridge - Other (Email, telephonic notification lists) Involve appropriate organizational divisions (business and technical) - 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 If not already established, create contact and escalation procedures for all significant events.	NRIC BP 0561, 0598, 0609, 8068	Changed
7-7-8556	**Recovery from the Absence of a Monitoring Requests Policy:** In the absence of a monitoring request polity, Service Providers and Network Operators should refer all communications intercept requests to corporate counsel.	Dependency on NRIC BP 8031, 8069	Changed
7-7-8557	**Recovery from Lack of Security Reporting Contacts:** If an abuse incident occurs without reporting contacts in place, Service Providers and Network Operators 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.	NRIC BP 8070	Changed
7-7-8559	**Recovery from Lack of IDS/IPS Maintenance:** In the event of a security threat, Service Providers and Network Operators 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).	NRIC BP 8072	Changed

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8561	**Recovery from Denial of Service Attack - Target:** If a network element or server is under DoS attack, Service Providers and Network Operators should evaluate the network and ensure 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.	NRIC BP 8074	**Changed**
7-7-8562	**Recovery from Denial of Service Attack - Unwitting Agent:** If an infected (zombie) device is detected, Service Providers and Network Operators 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).	NRIC BP 8075	**Changed**
7-7-8563	**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.	NRIC BP 8076	**Changed**
7-7-8564	**Recovery Incident Response (IR) Post Mortem Checklist:** After responding to a security incident or service outage, Service Providers and Network Operators should follow processes similar to Appendix Z, to capture lessons learned and prevent future events.		**Changed**
7-7-8565	**Recovery from Authentication System Failure:** In the event an authentication system fails, Service Providers, Network Operators, and Equipment Providers 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.		**Changed**

NRIC VII FG2B Cyber Security Best Practices
11/03/2004

NRIC VII Best Practice Number	NRIC VII Best Practice	NRIC VII BP Reference/Comments	NRIC VII (New/Changed/ Unchanged/Deleted)
7-7-8566	**Recovery from Unauthenticated Patching Systems.** Service Providers, Network Operators, 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.		**Changed**
7-7-8567	**News Disinformation after Recovery:** Service Providers, Network Operators, 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.		**Changed**

APPENDIX X. COMPUTER SECURITY INCIDENT RESPONSE PROCESS

BACKGROUND

Computer security events happen on a regular basis and organizations must be prepared to respond in a timely and appropriate fashion. The intent of this document is not to proscribe a specific set of responses but rather to outline the associated processes. While a number of the steps will be presented in a linear fashion, there may be opportunities to conduct steps in parallel. There are also a number of administrative and managerial issues that need to be considered separate and apart from the actual technical response. Wherever possible, organizations should plan for and consider their response to significant computer security events as part of the Disaster Recovery Plan. Organization with critical networked resources should establish a detailed computer security incident response plan as part of the Business Continuity Planning process. Organizations with a significant investment in or reliance upon their network(s) should consider the creation of a Computer Security Incident Response Team.

1. INITIAL RESPONSE
    a. Despite the views of individual security engineers, the principle objective of an incident response plan is to ensure business continuity and to support disaster recovery efforts. The scope and nature of any response must be consistent with the fundamental objectives of the business.
    b. As with any crisis, the initial response to a computer security event involves a rapid assessment of the situation and the execution of a number of "immediate action" steps designed to contain the problem and limit further damage.
        i. Upon detection of a suspected security event, notifications should be made in accordance with an organization's security response plan. At a minimum, IT and the affected operational units should be notified immediately. An incident handler should be identified to assess the situation and direct the initial response. If the organization has a Computer Security Incident Response Team they should be notified of the event and if appropriate, assume control of the investigation and response.
        ii. There are two issues that need to be addressed immediately. First, is the compromised system an immediate threat to external resources or critical internal resources, and second, are malicious processes running which could result in a substantial loss of data on the compromised system? As a general rule, systems that pose an immediate threat to external entities or critical business functions should be isolated from the network. Depending on the network architecture and available resources, this may mean physical isolation (i.e., removal of an Ethernet cable or phone line) or logical isolation, through the use of firewalls and routers. If a malicious process that could result in substantial loss of data appears to be running on the compromised system, the system should be immediately disconnected from the power source. In routine situations, the decisions to isolate and/or

power down the potentially compromised system should be made as part of the investigative process. Systems supporting life-support or mission critical functions should only be disconnected after careful consideration of the risks and under the direction of the proper authorities. Once the initial decision to isolate and/or unplug the device has been made, a more calculated analysis of the problem can take place.

2. INVESTIGATIVE PROCESS
    a. One of the first issues that should be resolved is determining the nature of the event. Where possible, non-malicious causes (i.e., software configuration errors and hardware failures) should be investigated and ruled out. Events determined to be non-malicious in nature should be documented and resolved in accordance with organizational policies. Where an obvious non-malicious cause cannot be identified, the incident should be responded to as a hostile event.
    b. Once a decision has been made to respond to the issue as a hostile event, the nature and intent of that response needs to be defined. If there is no desire to collect data for its intelligence or law enforcement value the incident can be responded to in much the same way as a non-malicious event. Since the extent and mechanics of the compromise will never be fully understood any system returned to service must be appropriately rebuilt, patched, and hardened before being connected to the network.
    c. Regardless of the organizational objectives (immediate return to service vs. investigation) some amount of initial data collection/preservation should be undertaken. Because the extent of the compromise is not known, this phase should be as non-alerting as possible. Logical steps to consider include:
        i. Review and analysis of the initial indicators of compromise
        ii. Inventory of operating system and applications/services (version and patch level)
        iii. Preserve and review system/application logs (copy to secure offline media)
        iv. Preserve and review security device logs (copy to secure offline media)
        v. Non-confrontational interviews of system administrators and users (as indicated)
        vi. Examination of other hosts on the network segment or hosts that share a trust relationship
        vii. Organizations not engaging in a full investigation may be able to infer the factors that led to a compromise from the limited data collected during this phase of the response. Organizations engaging in an investigation will use this data along with data collected during subsequent steps to develop an understanding of the vulnerability, exploit, and actions of the intruder.

d. Once the decision has been made to investigate an event, an organization must address a series of questions that will influence both the nature and the cost of the investigation.
    i. The fundamental issues that need to be addressed include referring the matter to law enforcement (this issue should be considered at the outset and periodically during the course of an internal investigation), conducting the investigation with in-house resources, contracting the task out, or working collaboratively.
    ii. The issue of responding immediately vs. monitoring the situation to develop additional information about the intruders, their methodologies and objectives must also be resolved. Before making a decision regarding any of these issues investigators should consult with management, the affected stakeholders, and their advisors (to include legal and PR).
    iii. If criminal activity is suspected, organizations should consider a referral to law enforcement agencies. Typically, events which result in significant financial loss (as measured by both opportunity costs and recovery costs), loss of life or potential loss of life, attacks on critical infrastructure, or which have the potential to cause widespread loss should be presented to law enforcement. As with any criminal matter, the threshold on law enforcement involvement will vary by jurisdiction. Organizations approaching law enforcement should be prepared to provide as much information as possible on the costs and impact of the event. While law enforcement is frequently better equipped to investigate a computer security event than an organization with limited technical or financial resources there are some operational and PR issues to consider. Once law enforcement joins the investigation, they have the discretion to dictate both the pace and objectives of the investigation however, law enforcement is typically sensitive to the business operations of the victim. Establishing good pre-existing working relationships with local Law Enforcement and fostering an attitude of trust and cooperation can mitigate this risk.
    iv. If a matter is being investigated internally, a decision needs to be made on whether to use in-house or contract investigative resources. Intrusion investigations can be technically complex and very time consuming. Organizations intending to pursue legal remedies should evaluate the technical skills, tools, and methodologies available in-house to ensue their legal options will be preserved. Organizations with a dedicated computer security team or those that do not intend to pursue legal remedies may find that their in-house technical resources are sufficient to conduct the investigation.
    v. Be aware that any data intended for use in criminal prosecution must be gathered carefully and according to strict evidentiary rules which can vary by jurisdiction (see below).
e. Determination to Restore or Monitor

i. A key issue that needs to be considered at the outset of an investigation is whether to immediately restore the system to a secure and operational state or monitor the system in an attempt to collect additional information on the scope and nature of the compromise. For most organizations, the initial reaction is to restore the system to a secure state and return to normal operations as soon as possible. Situations where organizations may want to consider monitoring before overtly responding include suspected involvement of an insider, suspected cases of corporate espionage, or cases of extortion.

ii. Once the decision has been made to monitor a system, safeguards must be implemented that allow for rapid response should the compromised system begin attacking external or critical internal resources or should a malicious process be activated that attempts to destroy valuable data on the system.
    1. Monitoring tools should be tuned to alarm on suspicious outbound traffic and someone should be tasked with immediately disconnecting the system from the network and/or power source if instructed to do so by the investigating team.
    2. The actual mechanics of monitoring will vary but will usually involve the use of a network sniffer and possibly an intrusion detection device.
    3. The typical objectives of monitoring a compromised system include identifying the source(s) of the intrusion, determining the mechanics of the compromise, identifying the goals/objectives of the intruder, and defining the true scope of the problem.
    4. In the course of monitoring hostile activity, additional compromised systems, to include systems external to the organization may be identified. Management will need to decide how and when to apprise those external organizations of the potential compromise. External notifications should only be made after coordination with organizational advisors to include legal and PR.

iii. At some point in the investigation, an assessment of the compromised system will have to be conducted. The specific tools and techniques will vary by operating system and event but the basic intent is constant; collect and analyze both volatile and non-volatile information from the system. Volatile data must be collected from the system prior to powering the device down. The volatile information of greatest interest includes a memory dump, a listing of active processes/applications and their associated network ports, active connections, and current users. The processes used to collect the data should be adequately documented and the data itself written to secure removable media (i.e., a floppy) or to an off-host (networked) resource. There are applications and system utilities available on most operating systems to collect this data however, an investigator should

assume that all applications on the system being examined have been compromised and cannot be trusted to return accurate information. Examiners should provide their own trusted tools that can be either run locally (statically compiled binaries run from removable media) or over the network. There are a number of limitations associated with examining data from a "live," potentially compromised system that are beyond the scope of this document to address.

f. Handling Digital Evidence.

i. A basic tenet of evidence handling is to maintain the item of evidence in its original state and to thoroughly document access to the item as well as the reason and process associated with any changes. With physical evidence, this dictates the order and type of examinations that can be conducted. The unique properties of digital evidence allow an examiner to avoid this issue. Using the proper tools, an unlimited number of identical copies of an item of digital evidence can be created for use by the examiner.

ii. The process of creating an evidentiary copy involves "bit level duplication" and there are a number of commercial and open source products available that can accomplish this task. The resources, experiences, and preferences of the examiner will dictate which tools are utilized. At a minimum, an examiner familiar with Unix-type operating systems can use the "dd" system utility to make forensically sound copies for subsequent examination.

iii. Critical to the process of creating an identical copy or "image" of a drive is ensuring that the original is not altered by the procedure and that each bit has been accurately recorded on the copy. Mounting the drive to be imaged as a "read-only" device can satisfy the first requirement while hashing algorithms such as MD5, which create a "fingerprint" unique to the input source, can be used to validate the copy process. The characteristics of the MD5 hashing algorithm are such that the alteration of a single bit in a file of any size will result in a different fingerprint. MD5 can be used to verify that the item of original digital evidence and any instances of Duplicate Digital Evidence (DDE) are identical.

iv. Whenever possible, the original item of evidence should be retained and used to generate a first generation DDE copy which is in turn used to generate all subsequent DDE copies. If the original evidence (i.e., production hard drive) cannot be retained as evidence, a first generation copy should be made and treated in the same manner as an item of original evidence would be. Forensic examinations should be conducted on subsequent generations of DDE.

v. Once the volatile information has been collected, a decision must be made whether to shutdown the system and "image" the drives or, to attempt to image the "live" system. For mission critical systems that cannot be taken off line, the system will have to be imaged while in

operation, potentially over a networked connection. In situations where the system can be taken offline, the original drives should be retained as evidence whenever possible. If the original drives cannot be retained the reasons should be documented. The actual process of creating a forensically sound copy will vary by tool and situation. Examiners unfamiliar with their chosen application should consult the documentation prior to attempting to image a drive or live file system. Once taken as evidence, access to the original drives, or 1st generation evidentiary copy, should be restricted. Any access to or transfer of custody over the physical article should be documented on a chain of custody form.

NOTE: Handling of digital evidence is a sensitive procedure. If the evidence is used in court, the opposing side will make every effort to show it was mishandled or otherwise rendered untrustworthy. This brief description of evidence handling should only serve as an introduction to the scope of the problem.

g. Data Analysis
    i. Once a suitable copy of DDE is available for examination, the analyst can use any number of commercial or open source tools to conduct the analysis. The analytical process should be thoroughly documented, to ensure defensible/repeatable results. The specifics of an examination will vary by incident but in general, an analyst will look for evidence of contraband files, unauthorized access to intellectual property, logs/indicators of hostile acts directed at or originating from the compromised host, and indicators of specific compromised resources (files, user accounts, and other systems). Investigators not employing a commercial forensic analysis tool will want to consider open source resources such as “ftimes” and “The @stake Sleuth Kit” (TASK) to support their analysis. Additionally, a number of vendors and security researchers (to include Sun and NIST) make hashes available for known good files. These resources can significantly enhance the quality and efficiency of a forensic examination by allowing an examiner to quickly categorize a significant number of files as “known good.”
    ii. If during the course of the examination evidence surfaces that indicates trust relationships were exploited the scope of the investigation may have to be expanded. If it becomes apparent the security of other organizations was compromised management should decide on the timing and nature of any notification. Depending on the circumstances, legal and PR should be consulted prior to the notification.

3. RECOVERY
    a. Once the volatile data has been captured and a forensically sound copy of the compromised device secured, work can begin on retuning the system to service. Because the true scope of a compromise often remains in doubt the

most prudent course of action is usually to rebuild the system from trusted media. Data should be restored from a trusted source and validated before being relied upon. The operating system and all applications should be updated wherever possible, patched, and all unnecessary services disabled. Organizations lacking security skills should consult any of the reputable and widely available resources dedicated to "hardening" servers and workstations. For purpose-built devices (i.e., routers, switches, and security appliances) consult the vendor for information on security-conscious configurations. All system passwords should be changed and hosts with which the compromised system shared a trust relation examined for possible signs of compromise. If the root cause for the compromise has been determined, appropriate steps should be implemented to mitigate the risks.

b. Network surveillance should be increased following an intrusion. Post-compromise monitoring of a network will often reveal additional probes and may help identify additional compromised resources.
c. Lessons learned from the investigation should be presented to management, and as appropriate, shared within the organization. Network and security policies should be reviewed and if necessary adjusted based on the findings of the investigation. To the extent resources permit, other resources on the network should be examined and hardened as necessary. Depending on the root cause, the network security architecture may need to be revised. If Incident Response procedures and or an IR team did not previously exist, consideration should be given to their establishment. Legal counsel should be briefed on the scope of the compromise and should provide an opinion on any obligation to report the event to customers, regulators or partners. Refer to the Postmortem process, Appendix Z.

APPENDIX Y. RESPONDING TO NEW OR UNRECOGNIZED ANOMALOUS EVENTS

This is a checklist to assist in responding to an anomalous event.

1. Investigate event, determine if malicious or non-malicious in origin (i.e., worm vs. configuration error or HW failure).
    a. If non-malicious resolve issue and document as appropriate
    b. If malicious or unknown, attempt to classify
        i. Determine if internal or external in origin
        ii. Determine if attempting to propagate
    c. Notify Security Response Team (SRT) and convene if appropriate
        i. Periodically Review need to convene SRT
2. Analyze available data sources
    a. INTERNAL
        i. Security Device logs
        ii. Bandwidth Utilization Reports
        iii. Netflow Data
        iv. Application and system logs
    b. EXTERNAL
        i. Security Discussion Sites
        ii. NIPC/CERT
        iii. Service Provider's Security Team
    c. PROACTIVELY COLLECTED
        i. If feasible examine hostile code Collect from:
            1. "honeypot"
            2. Compromised System
            3. Trusted external sources
            4. Consider making collected code and analysis available to Security Community
                a. Government Clearing Houses
                    i. CERT
                    ii. NIPC
                    iii. NCC/NCS
                b. Security/Networking Forums
                    i. NANOG
                    ii. SecurityFocus Discussion Lists
3. Respond
    a. Isolate compromised host(s)
    b. Where possible block malicious traffic with existing security devices
    c. Where available, apply expedient mitigation techniques (based on analysis of code)
    d. When possible, patch/harden to address specific issue being exploited
    e. Monitor network for signs of additional compromise
    f. Vendors- where appropriate, advise customers of mitigation/recovery options

   g. Providers – where appropriate, advise customers of mitigation/recovery options
   h. Reporting – If suspected criminal acts, report to Law Enforcement.
4. Recover
   a. Recover compromised hosts in accordance with DR/BCRS Plans
   b. Consider need to collect data for forensic analysis (See Appendix X)
   c. Survey infrastructure for other vulnerable hosts – patch/harden as appropriate
   d. Quantify loss if seeking legal remedies
   e. Monitor host and network for signs of subsequent compromise or exploitation
   f. Conduct post-mortem analysis
   g. Revise procedure and training based on Post-mortem analysis (See Appendix Z)

APPENDIX Z. INCIDENT RESPONSE POST MORTEM CHECKLIST

This is a checklist to capture lessons learned following an incident.

1. PREPARATION AND INFORMATION GATHERING
    a. Determine purpose of the investigation in order to ensure proper evidence steps are taken (e.g. Attorney Client Privilege, prosecution, etc.)
    b. Determine if law enforcement involvement is appropriate
    c. Determine various corporate groups that must be involved (Public Relations, Legal, Investigations, etc.)
    d. Document how the incident occurred, starting at discovery points of the incident (roadmaps and flowcharts as necessary)
    e. Develop inventory of all affected components, elements (hardware and software), business processes and people
    f. Identify data sources that will provide pertinent information that should be analyzed
    g. Collect data from identified sources and maintain per chain of custody requirements (if necessary)
    h. Develop timeline of incident events and IR activities
    i. Collect notes, interviews, conversations from various individuals involved in the IR
    j. Interview individuals involved in IR activities to determine events that occurred
    k. Enlist expertise based on technical needs and resource limitations
    l. Identify potential compromise of employee or customer personal data – ensure laws and regulations have not been broken/breached related to employee or customer personal data.

2. DETERMINE THE CAUSE (WHY) AND EFFECTS
    a. Develop data sources as necessary, such as filtering logs, IDS alerts, etc.
    b. Analyze and review data collected during IR activities
    c. Examine existing policies, processes and technologies
    d. Consult best practices and alert information
    e. Determine human errors and identify short cuts
    f. Identify employee misconduct and criminal misconduct
    g. Identify gaps and areas of non-compliance
    h. Involve necessary groups within company, including investigations, corporate compliance and HR
    i. Identify and resolve conflicting information
    j. Identify management issues resulting in acceptance of risk and bad management decisions
    k. Identify contributing factors and effects of the incident
    l. Determine if incident was intentional or accidental
    m. Identify if incident affected confidentiality, availability or integrity of key data and systems

n. Perform business impact analysis to quantify effect on customers, systems, and data, financial impacts to company (include investigation and recovery costs) and legal ramifications, in order to provide effective and efficient recommendations.

3. MAKE RECOMMENDATIONS AND FIX ISSUES
    a. Based on gaps, make recommendations for improvements to:
        i. Policies, standards and guidelines
        ii. Processes
        iii. People
        iv. Technology components
    b. Design and implement solutions as necessary
    c. Compile summary report to document the following:
        i. Post incident analysis
        ii. Summary of incident
        iii. Cause and effects
        iv. Actions performed
        v. Cost associated with response activities
        vi. Business impact of the incident
        vii. Lessons learned
        viii. Remediation actions required (recommendations)
        ix. Post mortem activities
    d. Report to all external entities as necessary