1200 G Street, NW
Suite 500
Washington, DC 20005

P: 202-628-6380
F: 202-393-5453
W: www.atis.org

September 25, 2012

VIA EMAIL
Jeffrey Goldthorp
Chief, Communications Systems Analysis Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Transmittal of NRSC Recommendations to Best Practices Modified by CSRIC II

Dear Jeff:

On behalf of its Network Reliability Steering Committee (NRSC), the Alliance for Telecommunications Industry Solutions (ATIS) hereby submits the attached document, which contains recommendations with regard to Best Practices that were significantly altered by the last Communications Security, Reliability and Interoperability Council (CSRIC II).

The NRSC recommends the proposals contained in the attachment be provided to CSRIC III for its review.

If there are any questions regarding this matter, please do not hesitate to contact me.

Sincerely,

Thomas Goode
ATIS General Counsel

cc: John Healy, Associate Division Chief, Cybersecurity and Communications Reliability Division

NRSC Recommendation	Number	CSRIC Best Practice	Reference	Original Wording
BP contains more than one concept. Consider separating into two or more BPs.	8-8-8106	Protect Wireless Networks 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. Employ up-to-date encryption capabilities available with the devices. In particular, vulnerable network and personal data in cellular clients must be protected if the handset is stolen.	IPSec. Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc. Dependency on NRIC BP 5018. NIST SP 800-40 v2.0 Creating a Patch and Vulnerability Management Program.	
BP contains more than one concept. Consider separating into two or more BPs. Last sentence calls to question if this is really a Best Practice. Always capitalize network roles for consistency (i.e., Network Operators).	8-8-8054	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.		
BP should end after "…danger of social engineering." in the first sentence. Move http "Source" to the reference section and eliminate bullet and six numbered items.	8-8-8773	Social Engineering: Network Operators, Service Providers and Equipment Suppliers should establish policies in preventing socially engineered attacks, but perhaps the most important step is educating employees to make them aware of the danger of social engineering. Source: http://www.windowsecurity.com/articles/Social_Engineers.html Social Engineering: Network Operators, Service Providers and Equipment Suppliers should establish policies in preventing socially engineered attacks, but perhaps the most important step is educating employees to make them aware of the danger of social engineering. Source: http://www.windowsecurity.com/articles/Social_Engineers.html • Training the front-line employees through case studies and understanding the need to recognize social engineering threats and its harmful consequences. The training must include: 1- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company. 2- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.	NIST: www.nist.gov Document is SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003.	
	8-8-8773 (cont'd)	3- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email. 4- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information). 5- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). 6- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).	NIST: www.nist.gov Document is SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003.	

New BP wording ok, but question whether should be a newly numbered BP, and old BP be maintained.	8-8-8026	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 sender and recipient, b) Does not depend upon secure transmission facilities, and c) Cannot be emulated by a non-trusted source.	NIST SP800-57 Recommendation for key management http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf.	SNMP Vulnerability Mitigation: Network Operators, Service Providers and Equipment Suppliers should apply SNMP vulnerability patches to all systems on infrastructure networks because SNMP vulnerabilities can create significant risk.
Remove reference as it does not add value. Correct spelling of "Blackberrys" in BP description.	8-8-8068	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 many of the following items as appropriate for your organization: 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.	Alternate broadband communication path for coordination and management.	
Replace Appendix X & Y with "NRIC VII FG2B Cyber Security Best Practices November 2004 Report, Appendix X. Computer Security Incident Response Process and Appendix Y. Responding to New or Unrecognized Anomalous Events". Add reference for Appendix X & Y: http://www.nric.org/meetings/docs/meeting_20041206/NRICVII_FG2B_December2004_BPs_Appendices.pdf, pg 55.	8-8-8061	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.	
Move last sentence of BP to reference section. Consideration should be given to determine if the cybercrime.gov link should be updated to "http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf." Replace Appendix X with "NRIC VII FG2B Cyber Security Best Practices November 2004 Report, Appendix X. Computer Security Incident Response Process". Add reference for Appendix X: http://www.nric.org/meetings/docs/meeting_20041206/NRICVII_FG2B_December2004_BPs_Appendices.pdf, pg 55.	8-8-8554	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 of the NRIC VII, Focus Group 2B Report Appendices.	IETF RFC3227, www.cybercrime.gov.	
Reword number 4 to say:"Create a common mailbox name and disseminate." Move the reference to RFC 2142 to the reference section and include link www.IATF.org.	8-8-8557	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) understands the security referral and escalation procedures. 3) Disseminate security contacts to industry groups/coordination bodies where appropriate. 4) Create e-mail IDs per rfc2142 and disseminate.		
Update IATF.net link to IATF.org in reference section.	8-8-8514	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 after the threat has been mitigated.	IETF rfc3013 sections 4.3 and 4.4. NANOG ISP Resources. www.IATF.net.	

Research applicable "system resource quotas" and include examples in the reference section. Research IETF RFC2350 and SEI-98-HB-001 and determine if they are relevant to the BP; if not, remove from reference.	8-8-8515	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 enforce system resource quotas.	IETF RFC2350, CMU/SEI-98-HB-001.
Reword to: Service Providers and Network Operators, when responding to security incidents or service outages, should follow processes similar to those outlined in Appendix X to capture lessons learned and prevent future events. Add reference for Appendix X: "NRIC VII FG2B Cyber Security Best Practices November 2004 Report, Appendix X. http://www.nric.org/meetings/docs/meeting_20041206/NRICVII_FG2B_December2004_	8-8-8564	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 those outlined in Appendix X to capture lessons learned and prevent future events.	ETF RFC2350, CMU/SEI-98-HB-001
Remove reference as it is redundant. Replace Appendix Y with "NRIC VII FG2B Cyber Security Best Practices November 2004 Report, Appendix Y. Responding to New or Unrecognized Anomalous Events". Add reference for Appendix Y: http://www.nric.org/meetings/docs/meeting_20041206/NRICVII_FG2B_December2004	8-8-8551	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 of the NRIC VII, Focus Group 2B Report Appendices.	Cross reference with 7-7-8551 developed under NRIC.
Remove reference as it is redundant.	8-8-8553	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 USCERT (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.	Cross reference with 7-7-8553 developed under NRIC.
Include "ietf.org" after IETF RFC3013, and update existing link to "www.nanog.org"	8-8-8513	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).
Remove the revision number from the reference section as well as the cross reference.	8-8-8032	Patching Practices: Service Providers, Network Operators, and Equipment Suppliers should design and deploy a well-defined patching process based on industry recommendations, especially for critical OAM&P systems. These processes should be based on the Software Patching Policy.	Configuration guide for security from NIST (800-53 Rev. 3). 'http://www.atis.org/ - ATIS-0300276.2008 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane; March 2008. Cross

Revise second sentence in BP: "Local logon of a system administrator should only be used in a situation of absolute necessity or emergency." Remove DOD document version and release number from reference.	8-8-8113	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 for troubleshooting or maintenance purposes. Some systems differentiate a local account database and network-accessible, centralized account database. Users should be authenticated via a network-accessible, centralized account database, not a local accounts database.	Department of Defense Telecommunications and Defense Switched Network Secuirty Technical Implementation Guide (Version 2, Release 3). 'http://www.atis.org/ - ATIS-0300276.2008 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security
Determine availablity of NSTAC report and provide reference.	8-8-8079	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 bruteforce 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/ - ATIS-0300276.2008 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: March 2008.
Multiple ideas and Best Practice is too long; break into separate, shorter BPs.	8-8-8522	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:	

	8-8-8522 (cont'd)	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 system 3.b. Confront user regarding personnel/HR policies. Ensure user does not have access to network 3.c. Disconnect system from network before allowing user access. 3.d. Request permission to examine system (see evidence/forensic procedures section if permis 3.e. If permission to review system is denied, follow-up with Legal/HR about the disposition of th 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 req 4.b. If security monitoring and awareness procedures adequately protect organization.	
Update language to conform with the BP tutorial (e.g., "Service Provider and Network Operator should...)	8-8-8507	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/ - ATIS-0300276.2008 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: March 2008 ISF CB63.
Refer BP to CSRIC II WG2A, as the reference in this BP appears in other BPs generated in that WG (8008, 8506, and 8509) and determine if there is an available URL/reference for the document. If there is none available, remove reference to ISF SB52 from the reference section.	8-8-8005	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.
Spell out BCP/DR as "Business Continuity Planning/Disaster Recovery"	8-8-8132	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.	
Consideration should be given to determine if the CERT reference document still supports the Best Practice since it is not being maintained and is noted as historic. If no longer applicable, consideration should be given to determine if the Best Practice is still applicable given advancements in technology. Include link to "ietf.org" in the refernece section for the RFC references.	8-8-8048	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).
There are two separate ideas; create second BP after semi colon, with "Encourage..". Remove "funded' as it is irrelevant. Remove reference to interopability testing forums, as several may exist at any time.	8-8-8044	BGP (Border Gateway Protocol) Interoperability Testing: Service Providers and Network Operators should conduct configuration interoperability 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).

This is not a Best Practice, as no industry role is identified. Action appears to be for the end user.	8-8-8025	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. ITU-T Rec. X.1051.
Remove "for redundancy" in the second sentence of the BP. Determine if there is an available URL/reference for the ISF SB52 document. If there is none available, remove reference to ISF SB52 from the reference section.	8-8-8506	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.	ISO 27002 Information Security Standards - 13.2.2 Learning from information security incidents ISF SB52.
Two sentences are redundent, suggest: Harden Default Configurations: Equipment Suppliers, relevant government agencies (e.g. US-CERT), and Network Operators should work together to identify default settings which may introduce vulnerabilities and provide guidelines on system deployment to ensure initial configurations are as secure as allowed by the technology. Drop reference as it refers to itself.	8-8-8004	Harden Default Configurations: Equipment Suppliers should work closely and regularly with 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.	Cross reference with 7-7-8004 developed under NRIC.
Remove ISP-ISAC as it does not exist and change Telecom-ISAC to NCC-ISAC. Inlcude URL to "http://www.ncs.gov/services.html#isac" in the reference section.	8-8-8066	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.	