1200 G Street, NW
Suite 500
Washington, DC 20005

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

July 12, 2013

Via Email
Jeffery Goldthorp
Chief, Communications Systems Analysis Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Reconsideration Request 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 proposals to revise several existing Best Practices not previously modified by the Communications Security, Reliability and Interoperability Council (CSRIC). The NRSC previously recommended that these Best Practices be modified, and is now providing specific text for the Commission's consideration.

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

In addition, ATIS staff discovered that Best Practice 8-7-0432 is truncated in both the ATIS and the Commission's database. The full version of the Best Practice Reference, as shown the second tab of the attached Excel spreadsheet, is as follows:

> *Enterprise MIBs are those written by vendors for their particular object. The managed object can furnish both standard MIB and enterprise MIB information. The standard MIBs are those that have been approved by the IAB (Internet Architecture Board, http://www.iab.org). Equipment and software vendors define the private MIBs unilaterally.*

To ensure the databases remain synchronized, ATIS requests that the Commission coordinate with ATIS to ensure that both databases are updated at the same time.

If there are any questions regarding these matters, please do not hesitate to contact me.

Sincerely,

Thomas Goode
General Counsel

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

NRSC Recommendations (June 2013)	NRSC New Best Practice Wording	BP Number	Existing Best Practice Description
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Network Operators and Service Providers should consult National Fire Prevention Association Standards for guidance in the design of fire suppression systems, and, when local zoning regulations require sprinkler systems, should seek an exemption for the use of non-destructive systems.	**8-7-0490**	Network Operators and Service Providers should consult National Fire Prevention Association Standards (e.g., NFPA 75 and 76) for guidance in the design of fire suppression systems. When zoning regulations require sprinkler systems, an exemption should be sought for the use of non-destructive systems.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Equipment Suppliers should make efforts, throughout a product's lifecycle, to minimize the possibility of having a silent failure on any system component, especially critical components.	**8-7-0557**	Equipment Suppliers should make efforts to minimize the possibility of having a silent failure on any system component, especially critical components. Equipment Suppliers should also constantly review the level of inspection and surveillance on critical components so silent failures are not able to manifest throughout the life of the product.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Property Managers should take the lead in restoration efforts of the base building infrastructure for an incident at a multi-tenant facility, ensuring that they have points of contact for each tenant to allow for coordination, support and additional resources as necessary.	**8-7-5236**	Property Managers should take the lead in restoration efforts of the base building infrastructure from an incident at a multi-tenant facility. Tenants should provide points of contact to the Property Manager to allow for coordination, support and additional resources as necessary.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Network Operators, Service Providers and Equipment Suppliers should use cables with adequate reliability and cable signal integrity, (e.g., flammability, strain reliefs, signal loss) and should mark as temporary and replace with standard cables as soon as practical any non-standard cables used because of an emergency restoration.	**8-7-5263**	Network Operators, Service Providers and Equipment Suppliers should use cables with adequate reliability and cable signal integrity. Such properties as flammability, strain reliefs and signal loss should be considered. If non-standard cables are used because of an emergency restoration, they should be marked as temporary and should be replaced with standard cables as soon as practical.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B. Note that NRSC recommends changing "Incident" and "Threat" to "breaches" to indicate that a recovery plan should account for a recovery problem.	Include Security Breaches in Business Recovery Plan: Network Operators and Service Providers should factor in potential security breaches of a plausible likelihood or significant business impact to their Business Recovery Plan.	**8-7-8131**	Include Security Incidents in Business Recovery Plan: A Network Operator's or Service Provider's Business Recovery Plan should factor in potential Information Security threats of a plausible likelihood or significant business impact.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Recover from Compromise of Sensitive Information Stored on Network Systems/Elements: Network Operators, Service Providers and Equipment Suppliers should conduct a forensic analysis when compromise or trust violations occur to determine the extent of compromise, revoke compromised keys, establish new crypto keys as soon as possible, and review crypto procedures to re-establish trust.	**8-7-8510**	Recover from Compromise of Sensitive Information Stored on Network Systems/Elements: When compromise or trust violations occur, Network Operators and Service Providers and Equipment Suppliers should conduct a forensic analysis to determine the extent of compromise, revoke compromised keys, and establish new crypto keys as soon as possible, and review crypto procedures to re-establish trust.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Recover from Misuse of Equipment for Remote Access of Corporate Resources: Network Operators and Service Providers should terminate VPN (Virtual Private Network) connections and issue a warning in accordance with the employee code of conduct if misuse or unauthorized use in a remote access situation occurs contrary to the AUP (Acceptable Use Policy), and, if repeated, revoke employee VPN remote access privileges.	**8-7-8521**	Recover from Misuse of Equipment for Remote Access of Corporate Resources: In the event of misuse or unauthorized use in a remote access situation contrary to the AUP (Acceptable Use Policy), Network Operators and Service Providers should terminate the VPN (Virtual Private Network) connection and issue a warning in accordance with the employee code of conduct. If repeated, revoke employee VPN remote access privileges.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Recovery from Authentication System Failure: Network Operators, Service Providers and Equipment Suppliers should, in the event of an authentication system failure, make sure the system being supported by the authentication system is in a state best suited for this failure condition (e.g., if the authentication system is supporting physical access, the most appropriate state may be for all doors to allow egress only; 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).	**8-7-8565**	Recovery from Authentication System Failure: In the event an authentication system fails, Network Operators, Service Providers and Equipment Suppliers should make sure the system being supported by the authentication system is in a state best suited for this failure condition. If the authentication system is supporting physical access, the most appropriate state may be for all doors that lead to outside access be unlocked. If the authentication system supporting electronic access to core routers fails, the most appropriate state may be for all access to core routers be prohibited.

FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	News Disinformation after Recovery: Network Operators, Service Providers and Equipment Suppliers should ensure that actions taken due to a spoofed, faked or distorted news item should be cross-correlated against other sources, that any actions taken should be 'backed out' and the previous state restored, and that news source authentication methods are implemented to ensure future accuracy.	**8-7-8567**	News Disinformation after Recovery: Network Operators, Service Providers and Equipment Suppliers should ensure that actions taken due to a spoofed, faked or distorted news item should be cross-correlated against other sources. Any actions taken should be 'backed out' and corrective measures taken to restore the previous state. News source authentication methods should be implemented to ensure future accuracy.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Network Operators, Service Providers, and Property Managers should implement fire resistance standards for key equipment locations (e.g., routers, central office switches, and other critical network elements) to reduce fires associated with DC power equipment.	**8-7-0622**	Network Operators, Service Providers, and Property Managers should use ANSI T1.311-1998 Standard for Telecommunications Environmental Protection, DC Power Systems for key equipment locations (e.g., routers, central office switches, and other critical network elements) to reduce fires associated with DC power equipment.
CSRIC III WG 8 Final Report recommended this BP for deletion and it was approved.		**8-7-0633**	Network Operators, Service Providers, Equipment Suppliers, and Property Managers should prohibit smoking in buildings.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Protect Authentication Files and/or Databases: Network Operators, Service Providers and Equipment Suppliers must protected authentication databases/files from unauthorized access, and back up and securely store these databases. MOVE THE FOLLOWING TO REFERENCE: Measures might include: 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.	**8-7-8083**	Protect Authentication Files and/or Databases: Authentication databases/files used by Network Operators, Service Providers and Equipment Suppliers must be protected from unauthorized access, and must be backed-up and securely stored in case they need to be 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.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Create Trusted PKI Infrastructure When Using Generally Available PKI Solutions: Network Operators, Service Providers and Equipment Suppliers should create a valid, trusted PKI infrastructure for digital certificates, using a root certificate from a recognized Certificate Authority or Registration Authority, assuring their devices and applications only accept certificates that were created from a valid PKI infrastructure, and configuring their Certificate Authority or Registration Authority to protect it from denial of service attacks.	**8-7-8084**	Create Trusted PKI Infrastructure When Using Generally Available PKI Solutions: When using digital certificates, Network Operators, Service Providers and Equipment Suppliers should create a valid, trusted PKI infrastructure, using a root certificate from a recognized Certificate Authority or Registration Authority. Assure your devices and applications only accept certificates that were created from a valid PKI infrastructure. Configure your Certificate Authority or Registration Authority to protect it from denial of service attacks.
FCC should consider sending to CSRIC the proposed new Best Practices wording in Column B.	Conduct Risk Assessments to Determine Appropriate Security Controls: Network Operators, Service Providers and Equipment Suppliers should perform a risk assessment of all systems and develop a security policy which recommends and assigns the appropriate controls to protect the systems, based on the value to the company.	**8-7-8089**	Conduct Risk Assessments to Determine Appropriate Security Controls: Network Operators, Service Providers and Equipment Suppliers should perform a risk assessment of all systems and classify them by the value they have to the company, and the impact to the company if they are compromised or lost. Based on the risk assessment, develop a security policy which recommends and assigns the appropriate controls to protect the system.