March 2011

Working Group 2A
Cyber Security Best Practices

Final Report

Table of Contents

1 Results in Brief

1.1 Executive Summary

Working Group 2A of the Communications, Security, Reliability, and Interoperability Council (CSRIC) is focused on addressing the Cyber Security Best Practices in the Communications Industry. "Communications providers and users are under constant assault from a collection of cyber criminals and others with even more malicious intent. While a large body of cyber security best practices was previously created by the Network Reliability and Interoperability Council (NRIC), many years have passed and the state-of-the-art in cyber security has advanced rapidly. This Working Group will take a fresh look at cyber security best practices, including all segments of the communications industry and public safety communities."[1]

With the advances in the network and equipment , CSRIC Work Group 2A structured itself to address Cyber Security Best Practices in five vertical (Wireless, IP Services, Network, People, and Legacy Services) and four horizontal areas (Identity Management, Encryption, Vulnerability Management, and Incident Response). It is no surprise with the changes in technology over the past five years that 41% of the 397 Cyber Security Best Practices are new, 41% are modified NRIC VII best practices, and only 18% of the NRIC VII best practices remained the same.

These Best Practices continue the theme stated more than ten years ago by the first NRIC: "The Best practices, while not industry requirements or standards, are highly recommended. The First Council stated, "Not every recommendation will be appropriate for every company in every circumstance, but taken as a whole, the Council expects that these findings and recommendations [when implemented} will sustain and continuously improve network reliability." [2]

In light of the current state of urgency, Service Providers, Network Operators, and Equipment suppliers are encouraged to prioritize their review of these Best Practices and prioritize their timely, appropriate actions.

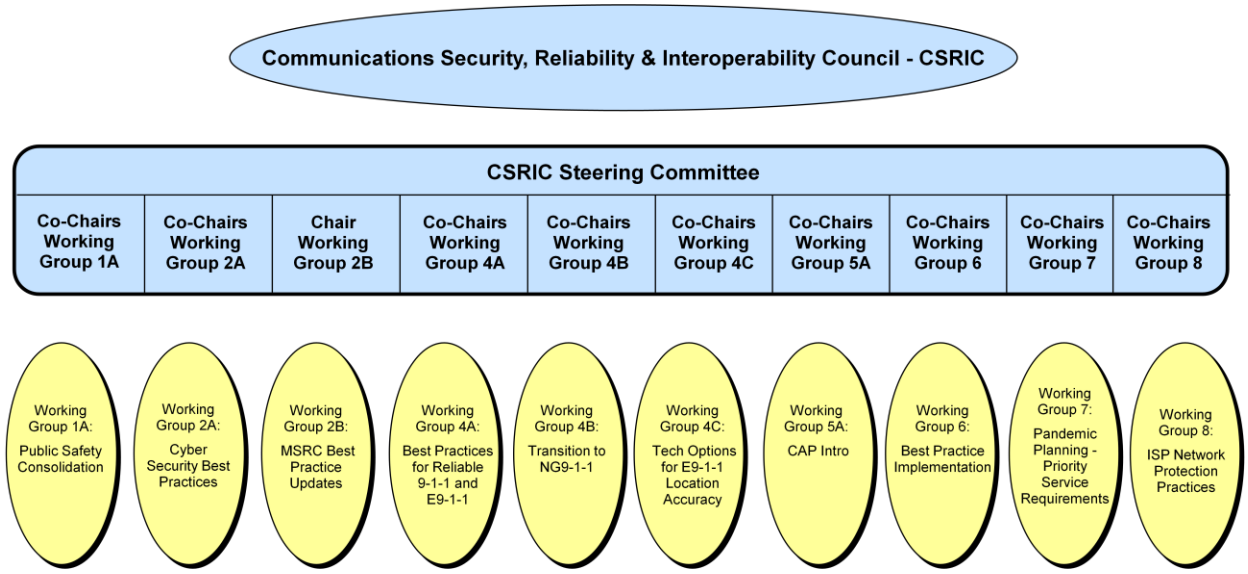
2 Introduction

The CSRIC was established as a Federal Advisory Committee designed to provide recommendations to the Federal Communications Commission (FCC) regarding best practices and actions the Commission can take to ensure optimal security, reliability, and interoperability of communications systems, including telecommunications, media and public safety communications systems. CSRIC created ten working groups, each with its own area of responsibility. Working Group 2A was charged with taking a fresh look at cyber security best practices across the communication industry.

[1] CSRIC Working Group Descriptions Source: http://www.fcc.gov/pshs/advisory/csric/wg-descriptions.pdf
[2] Best Practice Tutorial Source: http://www.bell-labs.com/USA/NRICbestpractices/tutorial.html

Malicious cyber activity is growing at an unprecedented rate, severely threatening the nation's public and private information infrastructure. In order to prepare for such attacks, it is incumbent upon the organization to know what needs to be protected. Working Group 2A began meeting in March 2010 to assess the Cyber Security Best Practices developed from NRIC VI and VII. Sub-Teams were commissioned into the five vertical and four horizontal areas (as mentioned above) to assess the NRIC Best Practices, eliminate obsolete or irrelevant best practices, identify gaps, and write additional best practices that are relevant for today's technology and infrastructure. While the best practices describe commonly-accepted practices and techniques to ensure the security of the network and systems, they are not overly prescriptive, allowing network service providers, operators and equipment suppliers enough latitude to make deployment decisions that best suit their business needs.

2.1 CSRIC Structure



2.2 Working Group 2A Team Members

Working Group 2A is comprised of thirty members, including its two Co-Chairs; Ed Amoroso of AT&T and Phil Agcaoili of Cox Communications. Members come from a wide variety of private and public entities, many of which possessed an extensive background in network and security. The FCC Liaison for Working Group 2A is Julia Tu.

Name	Company
Phil Agcaoili – Committee Chair	Cox Communication
Ed Amoroso – Committee Chair	AT&T
Rodney Buie	TeleCommunication Systems Inc.

Uma Chandrashekhar	TeleCommunication Systems Inc
John Coleman	NARUC
Doug Davis	CompTel
Martin Dolly	AT&T
Rob Ellis	Qwest
Fred Fletcher	ATIS
Chris Gardner	Qwest
Bill Garrett	Verizon
Rajeev Gopal	Hughes Network Systems
Allison Growney	Sprint Nextel
Barry Harp	US Department of Health & Human Services
Maureen Harris	NARUC
Robin Howard	Verizon
Dan Hurley	Department of Commerce
John Knies	CenturyLink
Micah Maciejewski	Sprint Nextel
Ron Mathis	Intrado
Brian Moir	E-Commerce Telecom Users Group
Jim Payne	Telecordia Technologies
Doug Peck	CA 911 Emergency Comm Office
John Rittinghouse	Hypersecurity LLC
Remesh Sepehrrad	Comcast Corporation
Monique Sims	L.R. Kimball / National Emergency Number Assoc.
Ray Singh	Telcordia Technologies
Jeremy Smith	L.R. Kimball / National Emergency Number Assoc.
Myrna Soto	Comcast Corporation
Gary Toretti	AT&T
Julie Tu	FCC Representative

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

In its December 2004 report, Focus Group 2B of the NRIC VII Council recommended 187 Cyber Security Best Practices. These practices stem from a review and update of the existing Best Practices from the NRIC VI Report from 2002 / 2003. For 2010 / 2011, CSRIC Working Group 2A's objective is to review the existing best practices with an eye toward modern network principals; determine the gaps, and ensure a comprehensive set of best practices are produced.

3.2 Scope

Problem Statement: Rapidly evolving and complex technologies in the communication industry are increasingly under attack from insiders, hackers, cyber criminals, and nation-states seeking economic advantage. Compromised technology or process controls can severely impact a company' brand and prowess impacting financials and shareholder value for many years.

Working Group Description: This Working Group will assess the existing best practices within the industry by:

- Analyzing existing NRIC, NIST, SANS, IEEE, etc. best practices related to Cyber Security
- Recommending modifications and deletions to those existing Best Practices
- Identifying new Cyber Security Best Practices across existing and relatively new technologies within the Communication industry.

Deliverables - Updated Cyber Security Best Practices reflective of the current technology environment within the Communications' Industry, and related references.

3.3 Methodology

3.3.1 Methodology Overview

Working Group 2A reviewed the 2005 NRIC VII Focus Group 2A recommendations for future cyber security focus groups to consider. These included:[3]

1. Voice over IP. "The focus group believes that future voice telecommunications will increasingly use this technology as network usage continues to converge between voice, video and data. This will include not only landline and broadband voice transmission, but also traditional wireless (e.g., cellular), voice, and data (e.g., wi-fi and WiMAX) networks.
2. Identity Management. "The need to correctly establish the authenticity of devices, humans and programs as they are used in network environments is becoming an increasingly critical issue."
3. Wireless security. "More and more endpoints in networking are migrating to a wireless environment whether via voice wireless networking or data wireless networking."
4. Blended attacks. "While basic definitions of what is a blended attack have been completed, the work of creating appropriate Best Practices to help deal with potential blended attacks is required." Blended attacks seeks to maximize the severity of damage by combining methods, for example using viruses and worms, while taking advantage of vulnerabilities in computers or networks.
5. Messaging security. "More and more operational components of networks are being managed by personnel who actively use various messaging products besides e-mail and voice communications."
6. Utility computing. "As telecommunications use increases, companies strive to improve their computational delivery systems; there is a large push towards the use of utility computing platforms (blade servers, networked storage, virtual network connectivity and virtual security product implementations)."

[3] NRIC VII FOCUS GROUP 2A Homeland Security Infrastructure Final Report
http://www.nric.org/meetings/docs/meeting_20051216/FG2B_Dec%2005_Final%20Report.pdf

7. Abuse Management. "In any area where technology is provided and where opportunists will attempt to take advantage of consumers and providers, there is the potential for fraud and abuse. While there are some Best Practices already provided that would start to help with the abuse problem, a great deal of additional work needs to be done to address the ever changing methods in which abuse and fraud are perpetrated on consumers and network providers."
8. Strategic outlook for Best Practices. "One area the focus group recognizes is that current Best Practices are predominantly addressing operational networks and do not provide guidance or focus towards overall strategic issues in cyber security."

Overall, Working Group 2A used a matrix approach in tackling the Cyber Security Best Practices for the Communication Industry. Utilizing the NRIC VII recommendations from above and given the vast array of new and innovative technologies over the past ten years, the group was divided into sub-groups to address the various functional areas. Groups met weekly or bi-weekly, assigned sub-topics to subject matter experts, researched best practices across a number of sources, evaluated the gaps to their existing environments, and developed modifications or additions to the existing Best Practices. This resulted in a recommendation of approximately 400 Cyber Security Best Practices.

3.3.2 Sub-Team Organization

Historically, Cyber Security Best Practices were heavily focused on network security. Working Group 2A performed an analysis of the key areas across the Communication Industry and a consensus was reach on nine key focus areas. These areas were divided into five key vertical focus areas which encompassed Wireless, IP Services, Network, People and Legacy Services and four key horizontal focus areas encompassing Identity Management, Encryption, Vulnerability Management, and Incident Response. Each focus area was assigned a sub-team lead based on expertise and interest. Additionally each working group member was asked to participate on two focus areas. The focus teams began meeting either weekly or bi-weekly in 2Q10 and expeditiously agreed on sub-topics for the focus area and assigned sub-topics based on expertise and interest.

The matrix below represents the five vertical focus areas. Team leads are highlighted. Team members and subtopics are listed in the matrix.

Wireless (1)	IP Services (2)	Network (3)	People (4)	Legacy Services (5)
WIFI **Bluetooth** **Mobile Devices** **Application Security** **Emerging Devices** **Wireless 3G, WiMAX, Microwave, & Satellite**	**Broadband** **Cloud Computing** **IPV6** **Voice over IP**	**Access Control** **Availability** **Confidentiality** **Integrity** **Security Mgmt** **Security Audit & Alarm** **Security Policy & Standard** **Recovery** **Intrusion Detection**	**Awareness** **SPAM** **Social Engineering** **Data Loss / Data Leakage** **Phishing** **Security Policy**	**Media Gateways** **Communication Assisted Law Enforcement (CALEA)** **Signal Control Points (SCP)** **Gateway to Gateway Protocol** **SS7**
Rodney Buie Micah Maciejewski Gary Toretti Bill Garrett	**Chris Garner** Jim Payne Ray Singh Barry Harp Bill Garrett	**John Knies** Doug Peck Rajeev Gopal Ron Mathis Jeremy Smith	**Fred Fletcher** Ramesh Sepehrrad Allison Growney John Coleman	**Robin Howard** Doug Davis Uma Chandrashekhar

The matrix below represents the four horizontal focus areas. Team leads are highlighted. Team members and subtopics are listed in the matrix below.

Identity Mgmt (6)	
Idm Lifecycle **Access Control** **Strong Authentication** **Certificates** **SAML** **Policy** **Password** **Role Base Access Control** **Systems Administration**	**Martin Dolly** Jim Payne Brian Moir Rajeev Gopal Ray Singh

Encryption (7) **Encryption Keys** **Cellular Networks** **Device Encryption** **Voice Encryption** **Data Encryption** **Key Management** **Key Recovery** **Cloud** **Standards**	**Dan Hurley** Ron Mathis John Rittinghouse Tim Thompson Jim Ransome Anthony Grieco Annie Sokol Bob Thornberry
Vulnerability Mgmt (8) **Alerting** **Risk & Vulnerability Assessment** **Mitigation** **Asset Inventory** **Patch Mgmt**	**Micah Maciejewski** John Knies Jeremy Smith Fernandez Francisco Rodney Buie
Incident Response (9) **Policy & Plan** **Prevention** **Attack Detection** **Response & Mitigation**	**John Rittinghouse** Barry Harp Robin Howard Myrna Soto Fred Fletcher

3.3.3 Sub-Group Approach

In 2Q10, each focus group began meeting individually to discuss the scope of the sub-group to determine the subjects to be addressed. If the area was covered in previous NRIC reports, the members decided whether to include the subject in this year's review. Additionally a gap analysis was performed on the existing topics to set the focus for the new work not addressed by the previous NRIC reports. Once each sub-topic was defined for the focus group, they were assigned to the sub-team members. Subject matter experts, utilizing focus team meetings and conference calls, examined existing Best Practices related to the focus areas and recommended changes and new Best Practices for their team. The analysis included:

- Elimination of obsolete or irrelevant Best Practices
- Updating references to outdated materials or web sites
- Identifying gaps and writing additional Best Practices

New Best Practices were vetted among the team at the meetings and through email. When the sub-group had completed its analysis, the completed document was forwarded to the Working Group Committee Lead. The Committee Lead combined all of the nine sub-group areas in to one document and assessed the document for duplicates and proper placement within each of the nine sub-teams. Recommendations were made to the Sub-team leads for moving or removing

items. After an agreement via a conference bridge or email, the final CSRIC Cyber Security Practices document was completed. It is attached as an appendix to this document.

4 Background

Security incidents from federal agencies are on the rise, increasing by over 400 percent from fiscal years 2006 to 2009.[4] The Poneman study reported "more than 83% of respondents believe that the individuals affected by a data breach lost trust and confidence in the organization's ability to protect their personal information. These perceptions often result in the loss of customer loyalty. In fact 80% of respondents in the PBI study reported that a certain percentage of data breach victims terminated their relationships with the organization."[5]

The importance of the communication infrastructure today is far-reaching to all aspects of our every day life domestically and internationally. As a society, we are reliant on the backbone communication "pipes" and wireless airwaves to get our information from "here" to "there", for purchasing items online, to "tweet" our everyday events, etc. However, malicious activity is growing at an alarming rate and threatens the world's public and private information infrastructures. Cyber risk is widespread and we must look to mitigate this risk if we are to maintain order and integrity. It is important to know where these threats are coming from and how to protect the networks and systems that provide much of the information flowing throughout the world today. What vulnerabilities make a device susceptible to an attack, fail, or create instability? Are these threats from the outside the organization or from employees / other internal people? How do we prepare to deal with a Cyber attack once it is already underway?

Interruptions to the networks and operations due to exploitation of these Cyber risks have become a common occurrence. Service Providers, Network Operators, Equipment Suppliers, and Government need to prepare for these situations and take action upon detection.

5 Analysis, Findings and Recommendations

5.1 Analysis

As discussed in Section 3, the Sub-Team Organization and Approach for Working Group 2A was distributed into nine Sub-Teams to expand the focus from the prior Council. The teams (in their first meeting) decided on the sub-topics that would be researched and analyzed by the sub-groups. Past NRIC topics were included as well as new technologies that evolved over the past five years. Each Working Group 2A sub-team decided within their team on the sub-topics to pursue for research and analysis.

1. Wireless

[4] GAO Testimony before the Committee on Homeland Security, House of Representatives. CYBERSECURITY GAO-10-834T

[5] Poneman, Larry, "privacy breach Index Survey: Executive Summary", Ponemon Institute, August 2008

   a. WIFI
   b. Blue Tooth
   c. Mobile Devices
   d. Mobile Device Application Security & Baselines
   e. Emerging Devices – Femtocells
   f. Wireless 3G, WiMAX, Microwave, & Satellite
   g. Wireless Device Vulnerability, Prevention, Data Loss / Leakage, Availability
2. IP Services
   a. Broadband
   b. Cloud Computing
   c. IPV6
   d. Voice over IP
3. Network
   a. Access Control
   b. Availability
   c. Confidentiality
   d. Security Audit & Alarm
   e. Security Management
   f. Security Policy and Standards
   g. Security Audit & Alarm
   h. Recovery
   i. Spam Controls
   j. Intrusion Detection & Prevention
4. People
   a. Awareness
   b. SPAM
   c. Data Loss / Leakage
   d. Social Engineering
   e. Phishing
   f. Security Policy
5. Legacy Services
   a. Media Gateways
   b. Communication Assistant Law Enforcement (CALEA)
   c. Signal Control Points
   d. Gateway to Gateway Protocol
   e. Social Engineering
   f. SS7
6. Identity Management
   a. Lifecycle
   b. Access Control
   c. Strong Authentication
   d. Certificates
   e. SAML
   f. Policy
   g. Password
   h. Role Base Access Control
   i. Systems Administration
7. Encryption

   a. Encryption Keys
   b. Cellular Networks
   c. Device Encryption
   d. Voice Encryption
   e. Data Encryption
   f. Key Management
   g. Key Recovery
   h. Cloud
   i. Standards
8. Vulnerability Management
   a. Alerting
   b. Risk & Vulnerability Assessment
   c. Mitigation
   d. Asset Inventory
   e. Patch Management
9. Incident Response
   a. Policy & Plan
   b. Prevention
   c. Attack Detection
   d. Response & Mitigation

5.2 Findings

1. Wireless

Security Providers, Network Operators, and Equipment Suppliers play a key role in ensuring the best practices (BP) are executed and met. Rapid changes in technology continue to evolve in the Wireless space, for example, five years ago, cellular phones were mostly used for their original design, making phone calls. With the introduction of "Smart" phones, a phone can perform as many functions as a PC. Applications are abundant and can allow a user to perform many day to day tasks, all from a device that fits into their pocket. The network continues to try to keep up with the demands. Home "cell towers" are now available for areas experiencing difficulties in receiving a signal and are now relatively inexpensive and available for the Consumer. With the increase sophistication in equipment comes concerns with securing and tracking the smaller devices, protecting the data, and preventing malware from infecting the devices. This is a key focus area that will continue to evolve.

For 2011, the Wireless Sub-Team analyzed the various aspect of the Wireless Industry and provided 47 new Best Practices (BPs) in this area, while modifying only 3 existing BPs and leaving 2 NRIC VII BPs unchanged.

2. IP Services

The IP Services area has grown dramatically over the past ten years. High speed broadband has expanded rapidly to the home and small business. With the proliferation of so many IP enabled devices, the industry needed to ensure the existence of an IP inventory for the future. Thus Internet Protocol Version 6 (IPV6) deployment and integration into all faucets of the technical environment is occurring on a rapid pace.

Voice over IP has also grown dramatically as most service providers offer reliable and integrated products with their broadband and IP TV offerings. Additionally, the newest platform service being offered under the title of "Cloud Computing" is quickly redefining the terms "network" and "perimeter". No longer is a company's perimeter completely contained within the company's facilities. Web applications, data, etc. may be hosted by a multitude of vendors around the world. This brings new definition to "perimeter security" where as application security, Identity Management / Access Management, and Data Security become equally or more important in protecting the integrity and privacy of companies customer information.

For 2011, the IP Services Sub-Team analyzed these critical items in the network, and provided 21 new Best Practices in this area, while modifying 7 existing BPs and leaving 2 NRIC VII BPs unchanged.

3. Network

The existing NRIC Best Practices were heavily focused on the network and network components (Network Elements, Element Managers, etc.) and lacking is the view of portable data and the leakage of data as a result of lost, misplaced or abandoned sources of sensitive data.

The existing NRIC Best Practices are valid and should remain in effect, however with the proliferation of the above mentioned portable devices new best practices have been identified and should become a part of the CSRIC Best Practices documentation.

For 2011, the Network Sub-Team analyzed these critical items in the network, and provided 23 new Best Practices in this area, while modifying 66 existing BPs and leaving 32 NRIC VII BPs unchanged.

4. People

The People Sub-Team began their analysis by reviewing the best practices as documented in the various NRIC reports, identifying new or additional best practices, and identifying best practices that are no longer applicable. The People Sub-team distributed their work across five focus areas:

Awareness – This area addresses the need for awareness to the components of cyber security for the enterprise, the employee and the customer.

SPAM – This area addresses the impact of spam on the ability of a network to perform at acceptable levels and identifies best practices for preventing network harm as a result of a spam.

Social Engineering – This area addresses the impacts of social engineering and how to prevent or minimize social engineering as a component of an attack on a network.

Data Loss/Data Leakage – This area addresses the issues and best practices associate with both data loss (normally from an external source) and data leakage (normally from an internal source) and the implications this has on cyber security.

Phishing – This area addresses the issues and best practices associated with Phishing. Phishing is the criminally fraudulent process of attempting to acquire sensitive information (i.e. usernames, passwords and credit card details) by masquerading as a trustworthy entity in an electronic communication.

For 2011, the People Sub-Team analyzed these critical items, and provided 20 new Best Practices in this area, while modifying 9 existing BPs and leaving 7 NRIC VII BPs unchanged.

5. Legacy Sub-Group

The Working Group 2A Legacy Sub-team reviewed the terminology related to in-scope Best Practices related to signaling, protocol, interoperability and security. It was clear that existing Best Practices that specifically documented SS7 network access control, authentication, DoS protection, network design, and link diversity should be modernized. With next generation signaling networks now being deployed, the need to provide industry Best Practices that provide convergence for legacy and next generation platforms was evident.

Media gateways (MG) were also reviewed. MG's perform translation functions between unrelated telecommunications networks such as the Public Switched Telephone Network (PSTN), Signaling System Seven (SS7), Voice-over Internet Protocol (VoIP) and provide control and signaling functions. VoIP to TDM media gateways covert TDM voice to a media streaming protocol. The Working Group 2A Legacy Sub-Team reviewed existing Best Practices related to Media Gateways for relevancy and long term evolution potential.

Lawfully Authorized Electronic Surveillance (LAES) Best Practices were also reviewed. Since the single existing Best Practice was created, the terminology has been updated to Communication Assisted Law Enforcement (CALEA). The Sub-Team recommended that the existing Best Practice be deleted and replaced with four new Best Practices developed to specifically address the CALEA issue.

Additionally Signal Control Points was reviewed and existing BPs were deleted and replaced with new proposed Best Practices that more appropriately addresses current industry practices.

For 2011, the Legacy Sub-team analyzed these critical items in the network, and provided 21 new Best Practices in this area, while modifying 7 existing BPs.

6. Identity Management

IdM functions and capabilities are used to increase confidence in identity information of an entity and support business and security applications (e.g., access control and authorization) including identity-based services. An entity is considered to be something that has separate and distinct existence and that can be identified in a context. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices.

In regards IdM standardization activities there are various level of maturity. Specifically, there are some standards specifications that are completed and there is a wide range of work that is still ongoing and still not matured. The approach taken is to focus on standards specifications that are currently available.

For 2011, the Identity Mgmt Sub-Team analyzed these critical items, and provided 8 new Best Practices in this area, while modifying 12 existing BPs and leaving 9 NRIC VII BPs unchanged.

7. Encryption

Because encryption plays a central role in cyber security, it is a logical topic for research, analysis and discussion in the work of CSRIC Working Group 2A. While it was relatively easy to identify those best practices developed during Network Reliability and Interoperability Council (NRIC) VII which address encryption and crypto-authentication, developing new best practices relating to encryption posed a greater challenge. The new candidate best practices address cloud computing, of growing importance and not addressed five years ago.

The challenge with the so-called “legacy” best practices dating back to NRIC VII was primarily to determine first whether they remained relevant and next to determine whether the references had been updated or supplemented. A related step involved determining whether certain best practices were more appropriately grouped with another sub-team’s work and vice versa.

For the new best practices, Encryption sub-team members identified topics that heretofore had not been described or presented as best practices. For 2011, the Encryption Sub-Team analyzed these critical items in the network, and provided 8 new Best Practices in this area, while modifying 7 existing BPs and leaving 4 NRIC VII BPs unchanged.

8. Vulnerability Management

Vulnerability Management continues to be a very challenging area due to the proliferation of zero-day exploitation of vulnerabilities, extensive malware infections from websites and spam mail and the general availability of Botnet tool kit targeted to "entry-level" hackers from the sophisticated attackers. Desktop / server security tools are ineffective in the battle to stop the spread of the malicious code. Zero day exploitation of the vulnerabilities leaves little to no time to address the multitude of patches that must be applied across the various platforms. This leaves service providers prioritizing only the high risk vulnerability exposures.

For 2011, the Vulnerability Sub-Team analyzed these critical items in the network, and provided 9 new Best Practices in this area, while modifying 15 existing BPs and leaving 9 NRIC VII BPs unchanged.

9. Incident Response

All organizations face interruptions to normal business processes. Assembly lines break down and the product stops moving from stage to stage. Machinery fails, supplies are late, documents are lost, whatever can happen, will eventually happen. Those organizations that rely on information technology (IT) systems face disruptions specific to information transmission, storage, and processing. The one challenge all organizations face is how to determine the cost of these interruptions. The ability to accurately forecast and budget for outages caused by security breaches continues to be a much desired business tool that has grown in importance as the reliance on information technology systems has grown. Also, the possible impact of data breaches continues to grow.

Most American businesses are not prepared to identify and quantify financial losses incurred during cyber events – nor are they properly structured to manage cyber security risk in general[6]. It would be impossible to foresee every possibility and therefore develop a formula that covers all events.

For 2011, the Incident Response Sub-Team analyzed these critical items in the network, and provided 7 new Best Practices in this area, while modifying 35 existing best practices and leaving 7 NRIC VII BPs unchanged.

5.3 Recommendations

CSRIC Working Group 2A recommends the attached set of 397 Best Practices across 9 focus areas (Wireless, IP Services, Network, People, Legacy services, Identity Management, Encryption, Vulnerability Management, and Incident Management) to the FCC for consideration of adopting the best practices for general use by industry. As threats become increasingly

[6] Unknown, "The Financial Management of Cyber Risk: An Implementation Framework for CFOs", Report pub. 2010 by the Internet Security Alliance, pp 39-46.

complex and persistent, network service providers, operators, and equipment suppliers must work together with increased diligence to secure the network infrastructure.

For future consideration, CSRIC Working Group 2A is recommends continuing research and discussion around the following areas:

Service Provider Network Protection

Malicious activity is growing at an alarming rate, threatening commercial and consumer networks and systems. Home users are particularly vulnerable because of a lack of knowledge about the threats and the tools that can help keep them safe on the internet. Trojans, Botnets, viruses, etc. continue to plague many of these devices and re-infecting them and other devices that communicate with the infected hosts. These devices normally connect to the internet via an Internet Service Provider (ISP). Therefore ISPs are aware of the infections and the type of malware circulating around the internet. The CSRIC Working Group 2A recommends that, where appropriate and possible, ISPs should detect and attempt to stop malware from traversing the internet while providing self help to the consumers who are infected from the malware. Working Group 8 examined this area and made recommendations for Best Practices. Working Group 2A believes this subject needs additional analysis since it is constantly evolving and recommends a new group should be formed with industry subject matter experts in malware detection, and remediation to assess other ideas and recommendations (such as a central clearing house for Blacklisted URLs).

Border Gateway Protocol (BGP) Recommendation

Several of the best practices mention or make reference to BGP (Border Gateway Protocol). This protocol, developed initially in June of 1989 with the publishing of RFC 1105, *A Border Gateway Protocol (BGP),* set in motion the practices through which IP networks interconnect and set the stage to become the Internet's exterior routing protocol of the future. There are 4 major revisions of BGP. BGPv1 (RFC 1105) BGPv2 (RFC 1162, June 1990) BGPv3 (RFC 1267 October 1991) and the final version of BGP 4 (RFC 1771, March of 1995). BGP's primary function is the exchange of network reachability information between networks (called autonomous systems), to allow each AS on an internetwork to send messages efficiently to every other interconnected network. Most (if not all) public IP space is interconnected with BGP. It is our recommendation that a new sub-group be formed with industry subject matter experts in BGP and inter-networking to formally address the needs of this vital part of our infrastructure.

IP Television / Video on Demand

Several Service Providers have begun offering services through which internet television services are delivered using the architecture and networking methods of the Internet Protocol Suite over a packet-switched network infrastructure. IPTV is distinguished from general internet-based or web-based multimedia services by its on-going standardization process and preferential deployment scenarios in subscriber-based telecommunications networks with high-speed access channels into end-user premises via set-top boxes or other customer-premises

equipment[7]. Video on Demand allows users to select and watch video or audio content on demand. Working Group 2A recommends future Councils analyze Best Practices in these areas as they mature in the coming years.

6 Conclusions

The CSRIC Working Group 2A spent more than nine months researching, analyzing, and evaluating Cyber Security Best Practices. During this time members participated in dozens of conference calls, met in various cities, identified gaps, and researched new Best Practices, plus dedicated countless hours editing and revising the final report.

In conclusion, members feel this Final Report is a fair and accurate representation of their collective view-points and perspectives and hopes this will help to improve Cyber Security through these Best Practices.

[7] Wikipedia, http://en.wikipedia.org/wiki/iptv

7 Appendix A – CSRIC Working Group 2A Reference List

- "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
- "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
- "Satellite Security" Online Journal of Space Communication, number 6 (Winter 2004) http://spacejournal.ohio.edu/issue6/main.html
- 2009 Carnegie Mellon University, Author: Mindi McDowell posted on: http://www.us-cert.gov/cas/tips/ST04-014.html
- 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.
- American National Standards Institute (ANSI) X9.9, X9.52, X9.17
- Anti-Spam Framework of Best Practices and Technical Guidelines, National ICT Security and Emergency Response Center, 2005
- ATIS Packet Technologies and Systems Committee (previously part of T1S1)
- ATIS Protocol Interworking Committee (previously part of T1S1)
- ATIS-1000030, *Authentication and Authorization Requirements for Next Generation Network (NGN)*
- ATIS-1000035, *NGN Identity Management Framework*
- Carnegie-Mellon Software Engineering Institute secure software development: http://www.sei.cmu.edu/engineering/engineering.html
- Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, 3GPP, 3GPP2, LTE, etc.
- Center For Internet Security (CIS Benchmarks)
- Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
- COBIT: http://www.isaca.org
- Combating Spam – Best Practices – Sendmail Whitepaper – March 2007
- Committee on National Security Systems Policy (CNSSP) 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, 20 March 2007
- Common Criteria: http://www.iso.org
- Configuration guides for security from NIST (800-53 Rev. 3)
- Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 263-294.
- Defense information Systems Agency (DISA) - VoIP0210, VoIP0220, VoIP0230, VoIP0245,VoIP0270
- Department of Defense Telecommunications and Defense Switched Network Security Technical Implementation Guide (Version 2, Release 3)
- doi.ieeecomputersociety.org/10.1109/MSP.2008.8
- draft-ietf-dhc-csr-07.txt, RFC 3397, RFC2132, RFC1536, RFC3118.
- Economic Espionage Act 1996

- Electronic Communications Privacy Act 1986
- Federal Information Processing Standards (FIPS) 140-2, PUB 46-3, PUB 74, PUB 81, PUB 171, PUB 180-1, PUB 197
- Garfinkel, Simson, and Gene Spafford. "Personnel Security". Practical UNIX & Internet Security, 2nd ed. Sebastopol, CA: O'Reilly and Associates, Inc. 1996. 389-395
- 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
- Graham-Leach-Bliley Act 2002
- Guide to Security for WiMAX Technologies (Draft)
- Health Insurance Portability and Accountability Act (HIPAA) 2001
- http://adsabs.harvard.edu/full/2004ESASP.558..243T
- http://blog.consumer-preference.com/2007/10/how-to-block-text-message-spam.html
- http://csrc.nist.gov
- http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf
- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
- http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-127
- http://en.wikipedia.org/wiki/E-mail_spam
- http://en.wikipedia.org/wiki/Mobile_phone_spam
- http://en.wikipedia.org/wiki/Public_key_infrastructure
- http://ezinearticles.com/?Employee-Security-Awareness&id=4084497
- http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security
- http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html
- http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Sharon.htm
- http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-HackerTactics.html
- http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Dolan.html
- http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html
- http://spacejournal.ohio.edu/issue6/main.html
- http://spamlinks.net/prevent.htm
- http://ssmo_home.hst.nasa.gov/SSMO_Best_Practices_010705/best%20practices.htm
- http://standards.ieee.org/getieee802/download/802.11w-2009.pdf
- http://wapedia.mobi/en/3GPP_Long_Term_Evolution
- http://www.3gpp.org/ftp/Specs/html-info/21133.htm
- http://www.aiaa.org/images/spaceops/SOSTC-BestPractices.pdf
- http://www.airspan.com/pdfs/WP_Mobile_WiMAX_Security.pdf
- http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/06/15/laptop-encryption-software-for-social-security-administration-telecommuters.aspx
- http://www.amazon.com/Hacking-Exposed-5th-Stuart McClure/dp/B0018SYWW0/ref=sr_1_1?ie=UTF8&s=books&qid=1251593453&sr=1-1
- 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

- http://www.atstake.com/services/smartrisk/application.html
- http://www.ca.com/files/whitepapers/data-loss-prevention-requirements-wp_203570.pdf
- http://www.csoonline.com/article/596163/mobile-phone-security-dos-and-don-ts?page=1
- http://www.cybercrime.gov
- http://www.cybersecurity.my/data/content_files/13/65.pdf?.diff=1176418561
- 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
  NIST SP 800-54 Border Gateway Protocol Security
- http://www.enisa.europa.eu/act/it/eid/mobile-eid
- http://www.fedcirc.gov/homeusers/HomeComputerSecurity/ Industry standard tools (e.g., LC4).
- http://www.gao.gov/new.items/d02781.pdf
- http://www.georgia.gov/vgn/images/portal/cit_1210/0/26/99359541Enterprise%20Information%20Security%20Charter%20PS-08-005.01.pdf
- http://www.ietf.org/rfc/rfc1321.txt
- http://www.ietf.org/rfc/rfc3882.txt
- http://www.imation.com/smb/laptop_data_protect.html
- http://www.inmarsat.com/Downloads/English/FleetBroadband/Getting_started/FleetBroadband_Best_Practices_Manual.pdf?language=EN&textonly=False
- http://www.k-state.edu/its/security/procedures/mobile.html
- http://www.linuxmagic.com/opensource/anti_spam/bestpractices
- http://www.microsoft.com/atwork/security/laptopsecurity.aspx
- http://www.rsa.com/products/DLP/wp/8738_PEDL_WP_0409.pdf
- http://www.sans.org
- http://www.scps.org/
- http://www.securityforum.org
- http://www.securityinnovation.com/pdf/security-awareness-best-practices.pdf
- http://www.sendmail.com/sm/wp/spam_best_practices/
- http://www.social-engineer.org/Newsletter/SocialEngineerNewsletterVol02Is07.htm
- http://www.sophos.com/security/best-practice/spam.html
- http://www.stonybrook.edu/nyssecure
- http://www.us-cert.gov/cas/tips/ST04-014.html
- http://www.usshortcodeswhois.com/
- http://www.windowsecurity.com/articles/Social_Engineers.html
- https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm
- https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Information Security Forum. "Security Audit/Review". The Forum's Standard of Good Practice, The Standard for Information Security. November 2000.
- International Organization for Standardization (ISO) 17799, 27002
- International Telecommunication Union (ITU) - CCITT Rec. X.700 (X.720) Series, Rec. X.800 Series, SS7 Standards, "Securing SS7 Telecommunications Networks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 5-6 June 2001, Rec. X.805, Rec. X.812, Rec. X.815, Rec. X.1051, X.1250, *Baseline capabilities for enhanced global identity management and interoperability*, Y.2702,

Authentication and authorization requirements for NGN release 1, Y.2720, *NGN Identity Management Framework* , Y.2721, *NGN Identity Management Requirements and Use Cases*

- Internet Engineering Task Force (IETF) RFC 2547, RFC 3813 & draft-ietf-l3vpn-security-framework-02.txt, RFC 2350, rfc3013 section 3, 4.3 and 4.4, RFC 3227, RFC 4942, RFC-1034, RFC-1035, RFC-2065, RFC-2181, RFC-2535, RFC-2870
- Internet Systems Consortium (ISC) BIND 9.2.1 US-CERT "Securing an Internet Name Server" (http://www.cert.org/archive/pdf/dns.pdf)
- ISP Resources. www.IATF.net
- 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
- 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
- Liberty Alliance Project, Privacy and Security Best Practices Version 2.0
- McClure, Stuart, Joel Scambray, George Kurtz. "Dial-Up, PBX, Voicemail, and VPN Hacking". Hacking Exposed, Network Security Secrets and Solutions, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 341-389.
- McClure, Stuart, Joel Scambray, George Kurtz. "Enumeration". Hacking Exposed, Network Security Secrets and Solutions, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 69-124.
- MPLS Forum interoperability testing (http://www.mplsforum.org).
- 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; "Secure Authentication Data as it is Entered". Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996
- National Security Agency (NSA) Security Configuration Guides; VOIP and IP Telephony Security Configuration Guides
- National Security Telecommunications advisory Committee (NSTAC) ISP Working Group - BGP/DNS
- 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
- Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Digital Signatures and Certification Authorities - Technology, Policy, and Legal Issues".
- NIIF Guidelines for SS7 Security.
- NIST 800-53 revision 3: Recommended Security Controls for Federal Information Systems and Organizations security control catalogue; NIST IR-7622, DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems; NIST SP 800-115 A Technical Guide to Information Security Testing and Assessment;NIST SP 800-119 (Draft) 2.4, (Draft) 3.5.6, (Draft) 3.6.2, (Draft) 4.2.3, (Draft) 6.5.2; NIST SP 800-40 v2.0 Creating a Patch and Vulnerability Management Program Dependency on NRIC BP 8034 and 8035; NIST SP 800-54 Border Gateway Protocol Security; NIST SP 800-63, *Electronic Authentication Guideline;* NIST SP 800-81 & SP 800-81 R1 Secure Domain Name System(DNS) Deployment Guide; NIST SP800-118 Guide to Enterprise

Password Management http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf; NIST SP800-14 Generally accepted principles and practices for securing IT systems. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf ;NIST SP800-57 Recommendation for key management http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf; NIST SP800-83 Guide to malware incident prevention and handling; http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf; NIST SP800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf; NIST Special Pub 800-12, Pub 800-14, Pub 800-26; NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII);* NIST Special Publication 800-53, Revision 3, Control Number PM-7 Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf; NIST: www.nist.gov Document is SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003; SP800-45 (NIST) http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf Guidelines on Electronic Mail Security

- North American Network Operators Group (NANOG) (http://www.nanog.org)
- Octave Catalog of Practices, Version 2.0, CMU/SEI-2001- TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf)
- Office of Management and Budget (OMB) Circular A-130 Appendix III.
- Organization for the Advancement of Structured Information Standards (OASIS), Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0
- PacketCable Security 2.0 Technical Report (PKT-TR-SEC-V05-080425); Security Specification PKT-SP-SEC-I11-040730, IETF RFC 3261
- RIPE-181, "A Route-Filtering Model for Improving Global Internet Routing Robustness" www.iops.org/Documents/routing.html
- Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 8 - 14.
- Sarbanes-Oxley 2003
- Schneier, Bruce. 1996. Applied Cryptography. 2d.ed. John Wiley & Sons.
- Secure Programming Educational Material at http://www.cerias.purdue.edu/homes/pmeunier/secprog/sanitized/
- Space Communications Protocol Standards (SCPS) Including ISO Standards 15891:2000 through 15894:2000 and related documents http://www.scps.org/
- Stopping Spam – Report of the Task Force on Spam – May 2005IS
- technet.microsoft.com/en-us/library/cc875806.aspx
- Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc.
- Telecommunications Act 1996
- 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.

- 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.
- USA PATRIOT Act 2002
- US-CERT "Securing an Internet Name Server"
- www.cert.org/archive/pdf/CSInotes.pdf
- www.cert.org/archive/pdf/def**cappellim**oore0804.pdf
- www.cert.org/security-improvement/practices/p072.html
- www.cert.org/security-improvement/practices/p096.html
- www.cio.ca.gov/OIS/Government/documents/ppt/insider-threat.ppt
- www.sans.org/reading_room/.../logrhythm-**monitoring**-may-2010.pdf
- www.**state**.**nj**.us/it/ps/
- www.us-cert.gov/GFIRST/abstracts.html

The Communications Security, Reliability and Interoperability Council - Incident Response Recommendations

CSIRC Incident Response Working Group for CY 2010

John W. Rittinghouse, Ph.D., CISM

Robin Howard

Fred Fletcher

Barry Harp

Leslie Peterson

Terry Dalby

Myrna Soto

Jorge Nieves

Aniket Bhardwaj

Contents

INTRODUCTION

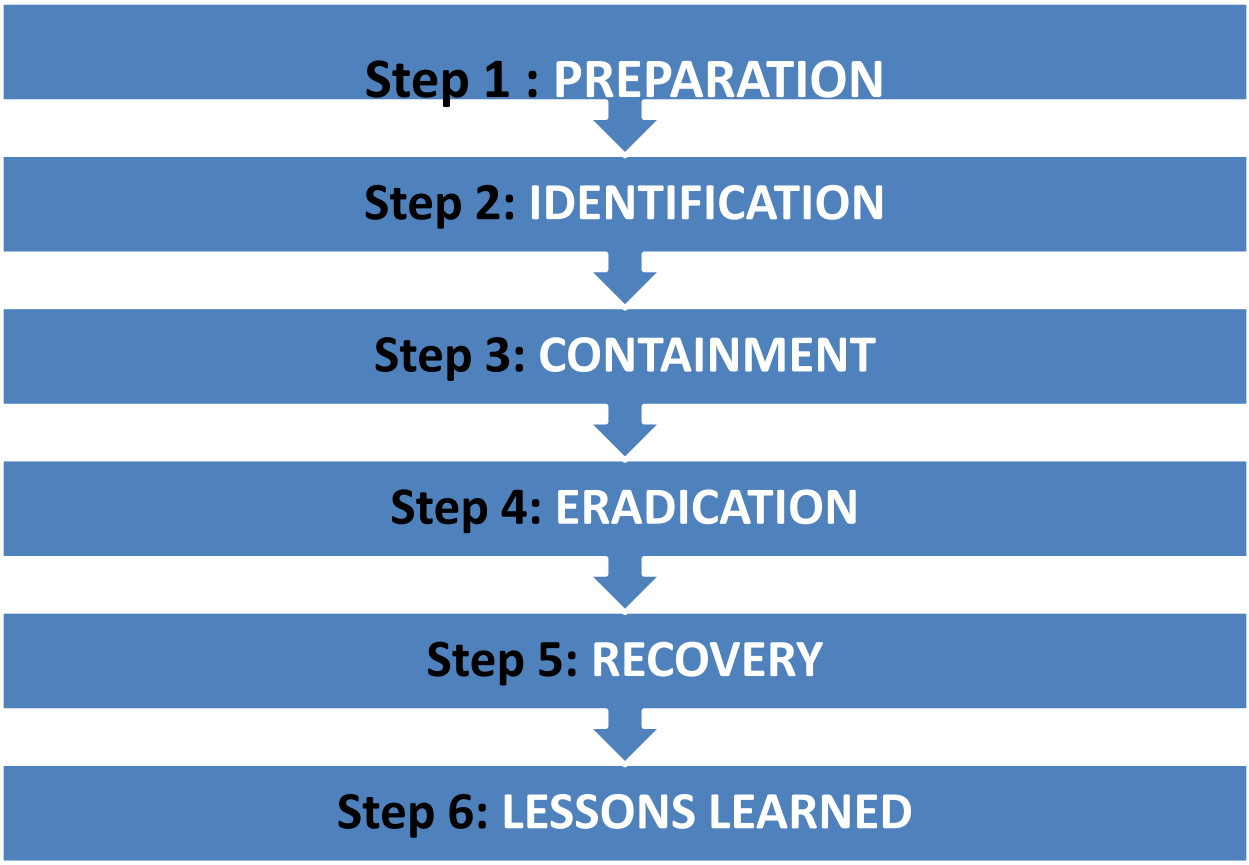
All organizations face interruptions to normal business processes. Assembly lines break down and the product stops moving from stage to stage. Machinery fails, supplies are late, documents are lost, whatever can happen, will eventually happen. Those organizations that rely on information technology (IT) systems face disruptions specific to information transmission, storage, and processing. The one challenge all organizations face is how to determine the cost of these interruptions. The ability to accurately forecast and budget for outages caused by security breaches continues to be a much desired business tool that has grown in importance as the reliance on information technology systems has grown. Also, the possible impact of data breaches continues to grow.

The results of a Ponemon study on the cost of privacy breaches provides further evidence of the importance of having a good quality incident response plan in place[1]. According to the study, "More than 83% of respondents believe that the individuals affected by the data breach lost trust and confidence in their organization's ability to protect their personal information. As we have found in our consumer studies on trust, these perceptions often result in the loss of customer loyalty. In fact, 80% of respondents in the PBI study reported that a certain percentage of data breach victims terminated their relationship with the organization."

In a more recent Ponemon Institute study[2], the cost of a data breach increased last year to $204 per compromised customer record. Also, the average total cost of a data breach rose from $6.65 million in 2008 to $6.75 million in 2009. A critical aspect of this study revealed that the management skills of the CISO, or an individual in an equivalent position, seemed to help hold down the cost of a data breach: The average per capita cost of an incident was $157 per record for companies with a CISO, versus $236 for companies without one. This brings up two important questions that businesses need the answers to in order to plan for the cost of these types of outages. What methodology can be followed to help management make informed decisions? What factors influence the final costs, both increasing costs and decreasing them?

[1] Poneman, Larry, "Privacy Breach Index Survey: Executive Summary", Ponemon Institute, August, 2008.
[2] Messmer, Ellen, "Data breach costs top $200 per customer record", Network World January 25, 2010, retrieved June 3, 2010 from http://www.networkworld.com/news/2010/012510-data-breach-costs.html.

Most American businesses are not prepared to identify and quantify financial losses incurred during cyber events – nor are they properly structured to manage cybersecurity risk in general[3]. A goal of this document is to discuss strategies to aid in creation of a methodology for dealing with interruptions so that normal activity returns as quickly as possible and costs are managed as required. It would be impossible to foresee every possibility and therefore develop a formula that covers all events. The discussion, then, should be around the general strategy used for managing interruptions. This general approach for Incident Response can best be seen in the following figure[4]:



[3] Unknown, "The Financial Management of Cyber Risk: An Implementation Framework for CFOs", Report pub. 2010 by the Internet Security Alliance, pp 39-46.

[4] Jim Murray, "Analysis Of The Incident Handling Six Step Process", Retrieved July 23, 2010, from http://www.giac.net/resources/whitepaper/network/17.pdf .

BEFORE YOU CAN PLAN YOU HAVE TO KNOW

Malicious cyber activity is growing at an unprecedented rate, severely threatening the nation's public and private information infrastructure. In order to prepare for such attacks, it is incumbent upon the organization to know what needs to be protected. Cyber-risk has become so widespread that governments are taking unprecedented steps to prevent possible insertion of malware into their telecommunications and information technology goods procured from outside sources. To that end, organizations need to have a plan to deal with the inevitable cyber-attack or incident.

Identify and Categorize Assets

The first step in preparing for an interruption is to identify those systems, resources, and processes that comprise the core of an organization's ability to sustain productivity and meet obligations. In other words, what can we absolutely not go on without? This is more than just an inventory process. It is extended by categorizing these resources so that a relative comparison can be made between multiple critical resources when conflicting and opposing demands arise. For example, a telecom business unit could identify two applications, app1 and app2, as being absolutely critical to its business objectives. During a serious interruption, management directs that these two applications be the first things restored, but there are not resources (system administrators, hardware, etc) enough to work on both applications at the same time. Which should receive priority? It would be better to have made this decision before the crisis rather than during the crisis.

Identify Threats

When looking to mitigate risks, it is important to know where threats are coming from. Once the critical assets have been identified and categorized, the next step is to evaluate what are the potential threats to these critical assets. What vulnerabilities in the assets make them susceptible to attack, failure or instability? Are these threats from the outside (external) or from employees or other internal people? Information like this can be invaluable in helping security officers and managers understand where risks may lie within their organizational infrastructure. Knowing that a possibility exists that an interruption to their delivery service could occur, managers can prepare for that situation and take action upon its detection. Not

only does this give security managers insight into where threats may come from, it helps them to prioritize which assets should be protected more than other organizational assets. These critical assets are identified for the purpose of lowering overall risk to the business or operation.

Threats are either malicious (intended to do harm, cause loss of income, value, reputation, etc) or non-malicious (accidents, equipment failures, misconfigurations causing outages). Some interruptions are non-malicious in that the person who introduces the threat into the organization did so by accident even if the originator of the threat meant it for mischief. An example would be the user who brought a virus or worm into the network. This user didn't intend to cause harm but the result might be just that.

What is the Risk to the Organization?

Risk related to the operation and use of information systems is another component of organizational risk that senior leaders must address as a routine part of their ongoing risk management responsibilities[5]. The Office of Management and Budget (OMB) Circular A-130, Appendix III, describes adequate security as security commensurate with risk. This risk includes both the likelihood and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. With the list of critical assets identified and an analysis of the threats against them, the user can begin to put some numbers down that represent the risk to the organization. In business, risk can be expressed as a dollar figure that represents the realistic cost due to the loss or interruption of an asset because of a specific threat. In other words, RISK = (Value of an asset * likelihood of a threat). If the value of the asset is high and the likelihood of a threat is high then the risk is high. As with assets, the conceivable list of threats should be ordered beginning with the most severe. This list should include all "likely" threats to all critical resources.

Evaluate Mitigating Factors

[5] NIST Special Publication 800-39 Draft, "Managing Risk from Information Systems: An Organizational Perspective", NIST, April 2008, pp 10. Retrieved 28 May 2010, http://csrc.nist.gov/publications/PubsSPs.html .

Mitigating controls are those technologies and processes that limit or lessen the impact of a potential threat. For example, in the case where a user brings a virus into the network, a mitigating control might include anti-virus software on the network. As with assets and threats, a list of mitigating controls should be considered when determining the overall risk posture of the organization. Accordingly, *"Organizations should ensure that there is close cooperation and collaboration among personnel responsible for the design, development, implementation, operation, and disposition of information systems and the information security professionals advising the senior leadership on appropriate security controls needed to adequately mitigate risk and protect critical mission/business processes.[6]"*

Develop a Plan

The natural outcome of the proceeding steps is to develop a plan to address likely situations. How should the organization respond when X occurs? What are the steps to be followed when Z happens and so on? What are the teams, processes, chain of command, service level agreements and so on that will help manage interruptions to assets. This is the type of incident response planning that helps organizations respond quickly and efficiently to potential interruptions. The plan, sometimes referred to as a protection strategy, should not be so broad as to have minimal guidance during real events or so narrow that it cannot provide the latitude to respond to specifics. To help protect organizations from the adverse effects of ongoing, serious, and increasingly sophisticated threats to information systems, organizations should employ a risk-based protection strategy[7]. Risk-based protection strategies are characterized by identifying, understanding, mitigating as appropriate, and explicitly accepting the residual risks associated with the operation and use of information systems[8]. A framework is clearly needed where many common questions would have previously been considered when not in the heat of the outage and pre-agreed upon decisions are offered as guidance to be considered in the event of a real event. Risk-based protection strategies are necessary to help ensure that organizations are adequately protected against the growing sophistication of threats to information systems. The serious nature of the threats, along with the dynamic environment in which modern organizations operate, demand flexible, scalable, and mobile defenses that can be tailored to rapidly changing conditions including the emergence of new threats, vulnerabilities, and technologies[9]. The first and foremost step in handling any incident is to be

[6] NIST Special Publication 800-39 Draft, "Managing Risk from Information Systems: An Organizational Perspective", NIST, April 2008, pp 20. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html .
[7] Ibid pp 23.
[8] Ibid.
[9] Ibid, pp 23.

well prepared, before it occurs, with a plan. Making procedural and "who to contact" decisions at the time when something actually transpires is not the right time at all. Here are a few recommendations to consider in preparing for the inevitable incident. A sample plan, as outlined by RFC 2350 is shown below.

RFC 2350 Incident Response Plan Template

1. Document Information

This document contains a description of an Incident Response Plan according to RFC 2350. It provides basic information about the IR Team, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 0.6 as of 2008/06/23.

1.2 Distribution List for Notifications

There is no distribution list for notifications as of 2008/02.

1.3 Locations where this Document May Be Found

The current version of this document can always be found at http://_____. For validation purposes, a GPG signed ASCII version of this document is located at http://_____. The key used for signing is the key as listed under Section 2.8 of this document.

2. Contact Information

2.1 Name of the Team

2.2 Address

2.3 Time Zone

2.4 Telephone Number

2.5 Facsimile Number

2.6 Other Telecommunication

2.7 Electronic Mail Address

Please send incident reports to: _____. Non-incident related mail should be addressed to: _____.

2.8 Public Keys and Encryption Information

Public keys for our team can be obtained from http://_____.

2.9 Team Members

The team leader is _____. Other team members, along with their areas of expertise and contact information, are listed in _____.

2.10 Other Information

2.11 Points of Customer Contact

The preferred method for contacting_____ is via e-mail. For incident reports and related issues please use _____. This will create a ticket in our tracking system and alert the human on duty. For general inquiries please send e-mail to_____. If it is not possible (or advisable due to security reasons) to use e-mail, you can reach us via telephone: _____. Our hours of operation are generally restricted to regular business hours. Please use our incident reporting form found at http://_____.

3. Charter

3.1 Mission Statement

The purpose of our IR Team is to coordinate security efforts and incident response for IT-security problems.

3.2 Constituency

3.3 Sponsorship and/or Affiliation

3.4 Authority

4. Policies

4.1 Types of Incidents and Level of Support

Our organization is authorized to address all types of computer security incidents which occur, or threaten to occur, in our Constituency (see 3.2) and which require cross-organizational coordination. The level of support given will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and available resources at the time. Special attention will be given to issues affecting critical infrastructure. We are committed to keeping our constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

We will cooperate with other organizations in the course of the IR process. This Cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities. Nevertheless we will protect the privacy of customers, and therefore (under normal circumstances) pass on information in an anonymized way only unless other contractual agreements apply. We operate under the restrictions imposed by applicable law. This involves careful handling of personal data as required by jurisdiction, but it is also possible that we may be forced to disclose information due to a Court's order.

4.3 Communication and Authentication

For normal communication not containing sensitive information we will use conventional methods like unencrypted e-mail or fax. For secure communication PGP-Encrypted e-mail or telephone will be used. If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. FIRST, TI, …) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident Response

We will assist the IT-security team in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

- Determining whether an incident is authentic.
- Assessing and prioritizing the incident.

5.1.2. Incident Coordination

- Determine the involved organizations.
- Contact involved organizations to investigate and take appropriate steps.
- Facilitate contact to other parties which can help resolve the incident.
- Send reports to other CERTs

5.1.3. Incident Resolution

- Advise the local security teams on appropriate actions.
- Follow up on the progress of the concerned local security teams.
- Ask for reports.
- Report back.

We will also collect statistics about incidents within its constituency.

5.2 Proactive Activities

- We try to raise security awareness.
- Collect contact information of local security teams.
- Publish announcements concerning serious security threats.
- Observe current trends and distribute relevant knowledge.
- Provide for community building and information exchange.

6. Incident Reporting Forms

There are no local Incident Reporting Forms available yet. If possible, please make use of the Incident Reporting Form of the CERT Coordination Center. The current version is available from: **http://www.cert.org/reporting/incident_form.txt**.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, we assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

Preparation

Preparation is one of the most important parts of the incident response process. Proper planning will provide the framework on which the incident handling team will operate and facilitate the "Command and Control" role during subsequent phases. The important preparation items are described in the following sections.

Setting an Organizational Policy for Incident Response

An Incident Response Policy should be documented which clearly states who is responsible for responding to an incident and setting the tone for the expectations of senior leadership. This policy should govern the general response, documentation and reporting of incidents affecting computerized and electronic communication resources, such as theft, intrusion, misuse of data, other activities contrary to an Acceptable Use Policy, denial of service, corruption of software, computer, and electronic communication-based HIPAA violations, and incidents reported by other institutions and business entities.

You need to establish a Security Incident Response Policy to protect the integrity, availability and confidentiality of confidential or proprietary information, including ePHI to prevent loss of service and to comply with legal requirements. This policy establishes the coordination of the organization's response to computerized and electronic communication systems incidents to enable quicker remediation, information gathering and reporting of infrastructure affecting security related events.

Develop and Formalize Incident Handling Instructions

Incident handling instructions are documents used by the incident handling team while they are about to begin the analysis or in the middle of the incident. The instructions act as a good resource for the team as most of the important aspects are present in the instruction manual. Because when the instruction manual is being prepared, the thought process is at its

best and chances are that most of the instructions are present in the document minimizing ad-hoc decision making during the incident. The key elements which help in preparing the instructions include Key Players which are discussed in the section below.

Contacts with Incident Handling Participants

The main part of the initial response is communicating with the right people and having a focal team lead or facilitate the Incident Handling process. There should be range of contacts to call upon, as needed, during the various stages of the response. The contacts should include Human Resources, Corporate Legal, Corporate Communications and a variety of technical groups (i.e., network, system and database administrators, etc.). These key players should be able to provide details like logs from firewalls, systems, routers and switches. These logs reveal a substantial amount of information which could possibly lead to the attacker or in the direction of making a conclusion.

Create an Incident Response Kit

Using a combination of various tools, it helps to follow up with an incident in a formalized manner. The importance and purpose of all the available tools should be well known in advance. Just like doctor's who carry a medical bag, the Incident Handling response team should have a set of tools or a kit available to them prior to an incident occurring.

TOOL (S)	PURPOSE
Response Kit	The response kit serves the purpose of containing all of the software, network and peripherals cables all in one place so that at the time of a real incident no item or tool is missed.
Forensics and Imaging	Various tools are available in market for handling evidence in a secure manner, capturing volatile data like running processes.
Intrusion Detection tools (IDS)	The IDS monitoring software serves as the window for viewing any possible signs of further attempted intrusion. The host based IDS (for end point protection) and network based IDS (network level protection) serve the purpose of viewing any signs of malicious activity.
Vulnerability assessment	The assessment tools should be in place so that after putting systems back online, they can be tested for any signs of future attacks. This ensures newly deployed systems are free from any vulnerabilities and helps in discovering any possible threats. It is important to ensure that all protection layers or key configuration controls of the system are reviewed (i.e., application, web, operating system, network ACL or firewall rules, etc.).

The SANS investigative toolkit is one example of a good resource[10]. The kit includes:

[10] http://www.sans.org/sift-kit/essential.php .

- Peripheral cables like USB, Parallel, Serial, Console;
- Network Cables (crossover & straight through);
- HUB's;
- Anti-static bags for evidence;
- Blank CD's for burning software from response laptop;
- Call list;
- Forensics software;
- Imaging software;
- A Laptop installed with the aforementioned software;
- Notebook with pen/pencil.

Incident checklist and communication plan

The primary incident response handlers should always carry incident checklist with them. Since it is a very stressful work, chances are that some important steps will be missed. So in order to avoid that situation, a checklist should be maintained. The communication plan should also be sound which should clearly describe, in what events the process should be escalated to other incident handlers. One of the members in the team should be charged with primary communicator to both management and within the team. This also keeps the management up to date with the latest developments. Any communication to external entities including media should be channeled through Legal and the Corporate Communications team.

Threat Modeling

For all anticipated types of attacks or security issues, a clear method of assessing the risks to the business should be available. This is the criteria used to make a decision on how impactful the issue is to the business (i.e., critical, high, medium, low risk, etc.). The priority given to the response will derive by the severity of the tag given to it.

Identify and Designate an Incident Response Team

There should be a team of individuals that are considered the focal point for handling any kind of incident which an organization might encounter. The skills of the individuals should be of prime consideration and should span many disciplines throughout the organization. Because the process of incident handling can be very stressful, the incident response team should have certain skill sets; in particular, they should be technically sound, having good

organizational and inter-personal skills. And it is always good that someone from the team knows various languages since there is a possibility of organization having offices in various geographical locations. The whole team should be diplomatic in nature because there are times when compromises need to be made and someone who can negotiate would be an added advantage.

Interruption Cost Considerations

All assets have value – intrinsic value, (the cost to acquire or produce it) and potential value (what money the asset can yield). If the organization is denied the asset, then the value of the loss can be based on the intrinsic value plus the potential value lost during the time the asset is denied. Various types of costs need to be understood before we can place value on an asset.

1. Lost asset costs – any time an organization loses an asset, especially an asset that is in production use, that loss costs money. Loss quantification can vary greatly depending on the type of business and the type of outage.
2. Loss of business income while the asset is unavailable – for example, if an organization that provides digital media services loses a device because of a cyber attack, a lightning strike, or a fire, that loss creates an outage that, in turn, will create customer dissatisfaction and possibly even a direct loss of revenue. If orders for pay per view services cannot be processed, there is direct loss of revenue. In this example, the organization may have to compare the number of orders that occurred during a previous time frame with the number of orders that could have occurred during the outage in order to quantify the loss.
3. Recovery costs (efforts to bring the asset back on line at least temporarily) – in the face of a cyber attack, many organizations take the approach of putting all hands on deck to put out the fire. The rationale for this, of course, is the more help you have solving the problem, the quicker it will be solved. With a cyber-attack, unfortunately, this is rarely the case. Responding to cyber attacks successfully requires a great deal of preventive measures be taken in order to properly mitigate the threat. The preventative costs that an organization would bear before an attack will almost always outweigh the “all hands” approach costs that are incurred after an attack.
    a. Alternative providers – when faced with outages, some organizations have taken preventative measures to have their services fall-back to outsource providers in order to avoid any interruption in business operations. Depending on the nature of the business, this may or may not be a suitable alternative. Each organization

has to weigh the costs of outsourced services against the costs of bearing the brunt of the cyber-attack. Even in the face of a cyber attack, where alternate providers are used, the affected organization still has to deal with cleaning up the effects of the cyber-attack. No organization walks away from a cyber-attack unscathed and certainly not without incurring unexpected, additional, unwelcome costs.

b. Temporary systems – the use of temporary systems as a substitute for those systems taken offline during the course of the cyber-attack is common practice. If a server goes down in today's modern operations environment, it can be taken offline and replaced with a virtual machine within a matter of a few minutes. More and more, organizations are relying on virtual instances to circumvent cyber attack scenarios. They are cost effective and relatively easy to implement. Using virtual instances helps reduce cost and lower risk when a cyber attack occurs.

c. Additional staff or facilities – in organizations where customer-facing activities are considered high volume operations, it is not uncommon to have staff identified on standby in case of an emergency. In the event of a cyber threat manifesting itself, often these staff members are called into action. When that happens, it costs an organization additional money in the form of resources (direct cost) and support for all those resources (indirect cost).

4. Remediation costs – often, the first measures taken by an organization are temporary measures. They are considered as band aids use to stop the bleeding until a more permanent solution is found. Sometimes this requires the purchase of additional equipment, bringing on additional resources with adequate skill sets to help solve the problem, or other measures as determined by the organization. Each of these additional steps of course cost more money to the organization.
5. Legal or contractual penalties - Where laws are typically tied to a state or region, cyber transactions occur in a realm without fixed borders, where information travels at the click of a mouse. No company is immune to the application of territorial laws to business conducted through Internet.
6. Brand damage or increased marketing costs due to interruption are another concern. How an organization communicates problems to the public often is the determining factor in their future success. The damage a cyber attack can cause to any brand should never be underestimated and the expense organizations have to incur in order to publicize and protect that brand can quickly become very large numbers. Many large organizations have seen their market value drop dramatically when they have suffered through a cyber attack. Any misstep in communication or in the incident response process can have long lasting negative effects.

It is important to point out that there is no magic in the paragraphs above. This is a standard risk-based approach to evaluating any situation. It is accurate to say that this process helps managers understand what truly is critical in their environment, to understand how it could be interrupted (at least the likely vectors) and, if it happens, what are the first steps in recovering from the situation. It has been suggested that without sufficient planning the costs will be much higher. There is one line of thought that contends 80% of companies that have no business continuity plan will fail within 18 months of a serious interruption to business. Some people claim this is over inflated but even so, the numbers are significant, ranging from 20-40%. But even if the company doesn't fail, the costs are always going to be higher and the losses greater without appropriate planning. As an example, let's consider the following situation. Some event is detected that makes operators suspicious. This event might be detected by a user report or by a technical system alert. In any case something is wrong and warrants further investigation. Typically, the investigation is simply answering a series of questions, similar to those shown below.

Troubleshooting Questions

- What are the symptoms of the problem?
- How extensive is the problem (scope – areas of impact)?
- Is it still active?
- Are we being attacked currently or is it just cleanup at this point?
- Can the problem be fixed immediately or are there viable work-a-rounds?
- Is there a permanent fix?
- Is it malicious?

The extent of the cost will depend upon the answers provided to the questions shown above. This is where prior planning pays its first great dividend. If the right response plan is in place, damage and loss to the asset can be effectively minimized. The quicker the response to the event the more likely the damage (and overall cost to the organization) will be lower. Most organizations try to adhere to some industry standards for network protection these days. Guidelines like ISO 27002 or NIST 800-53 and COBIT are frequently cited as baseline references for security. Because of the diverse nature of enterprise operations, it is difficult and often impossible to assume that every operation is going to perform incident response in the same manner.

Cost Considerations

In considering the types of costs used to calculate losses during any given stage of an incident response process, we need to look at direct costs, indirect costs and consequential costs. The direct costs we refer to herein include such things as the burdened cost of labor, equipment repair or replacement, etc. Indirect costs (referred to above as Interruption Costs) that we consider include organizational downtime factors such as loss of productivity, inability to sustain or continue operations, loss of sales, etc. Consequential costs are costs that are incurred after the incident has been resolved and are directly attributed to the incident itself. This may include an increase in customer churn, refusal to conclude a purchasing process, cancellation of services, the cost of defense against future litigation, etc.

One overlooked truth is that downtime costs accelerate in a non-linear fashion every hour. If a system fails for five minutes, the costs are fairly low because manual methods (paper and pencil) of making records or communicating by telephone instead of e-mails can suffice to conduct business. Over an extended period, however, the volume of work overwhelms the manual processes. Yet some businesses cannot run at all on manual processes. Business and financial operations increasingly deteriorate, and the rate of dollar loss grows — sometimes to the point of fatally damaging the business. In addition, when assessing the financial impact of downtime, it is necessary to consider factors such as potential lost revenue, reductions in worker productivity and damaged market reputation. In some cases, downtime can even reduce shareholder confidence, which can create unnecessary and unplanned costs. Financial analysts and accountants at the company can help come up with the list of relevant factors that are most affected by downtime and contribute most to its costs[11].

When Awareness of a Cyber-incident Occurs

Investigate the event in order to determine if it is malicious or non-malicious in origin (i.e., worm vs. configuration error or HW failure). In most organizations, the investigation begins after someone has reported a problem or a problem with network performance has been detected. Regardless of the manner in which an event is reported, it must be investigated. One of the first things that the investigating team needs to determine is an answer to the question

[11] Toigo, Jon William, ”Disaster Recovery Planning: 3rd Ed.”, Princeton, NJ, Prentice Hall PTR, 2003.

"How bad is it?", generally followed with an inquiry like "How long will it take to fix it?" At this point in the incident response process, any guess as to how long it will take to fix it is just that -- a guess! The well-trained security specialist can quickly determine whether or not an event is a nuisance or a malicious threat to the organization. In either case, calculating costs at this point simply comes down to time and money.

Time and money in this case equate to direct labor costs. Most of the steps that occur in determining what type of events you're dealing with and how bad the event is will almost always equate to direct labor costs. Having said that, one of the key factors to consider here is *"the person tracking costs must know when to begin accurately tracking the number of personnel that get involved in this incident as well as how to track the number of hours that they contribute to solving the problem*." In order for any level of accuracy to be taken seriously in calculating the cost of an incident, the person placed in charge of mitigating the events should know or be briefed on the importance of tracking the level of effort (i.e., man hours) used to resolve the issue. The most difficult part here is to look beyond the work being performed by the cyber security incident response team and account for efforts contributed by other department personnel towards resolving the cyber-incident or responding to the effects of the cyber-incident. For example, while the CSIRT may be performing work, IT personnel may be performing tasks such as network isolation, patch level reviews, or a myriad of other activities in order to respond to the incident. People in the marketing department may be coordinating with public relations teams and trying to put a positive spin on the incident or creating a press release to explain to the public what has happened. If the cyber security incident involved privacy data, the problem becomes even greater. Many states require notification processes be started immediately upon the detection of a cyber security incident that could result in the compromise of privacy data.

This is a dreaded situation for most companies because it forces them to go public with the issue and to take steps to mitigate any losses as a result of the compromised data being mishandled, misused or made public. This often results in lawsuits and general condemnation from the public. While it may be an overreaction, the effects are real and have devastating impact in the stock market. When one begins to consider all of the aforementioned, it is little wonder that many large corporations set up a war room to handle cyber security incidents as soon as they begin. In today's business environment, companies cannot afford to overlook anything that impacts their bottom line. The problems are not limited specifically to

corporations. Unfortunately, very few have meaningful or reliable metrics for their security controls. According to Sam Merrell at CERT, "*What gets measured gets managed.*[12]"

Many government agencies have been the victim of cyber attacks and have handled the situation poorly. Frequently, the urge to keep this situation quiet is the worst thing that could be done. Many times, managers fall victim to the temptation to try and solve the problem internally without letting it become a public matter of record. What happens more often than not is that an internal leak upsets their plans and they now have two disasters to fight – the cyber security disaster and a public relations disaster. For this reason, it is recommended the companies develop strict guidelines, metrics, and policies that deal with how their managers, executives, and employees react during the course of a cyber security incident. These guidelines and policies should become a part of a disaster recovery and business continuity plan that is periodically rehearsed. Numerous studies have shown that companies that fail to prepare for a disaster generally perform poorly in a disaster situation. Furthermore, that poor performance almost always leads to increased costs to the company. Lack of planning, lack of training and, most importantly, lack of preparedness are all compounding factors that make a bad situation even worse.

Reporting an Incident

A computer incident within the federal government as defined by NIST Special Publication 800-61 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Reports of computer incidents should include a description of the incident or event, using the appropriate taxonomy, and as much of the following information as possible; however, reporting should not be delayed in order to gain additional information.

According to the Federal Incident Reporting Guidelines, the minimum information to include in a report (to CERT) is as follows:

[12] Merrell, S., and Stevens, J., "The Confluence of Physical and Cybersecurity Management", Software Engineering Institute (SEI), Carnegie-Mellon University, Pittsburgh, PA, from a presentation given at GOVSEC 2009.

- Agency name
- Point of contact information including name, telephone, and email address
- Incident Category Type (e.g., CAT 1, CAT 2, etc., see table)
- Incident date and time, including time zone
- Source IP, port, and protocol
- Destination IP, port, and protocol
- Operating System, including version, patches, etc.
- System Function (e.g., DNS/web server, workstation, etc.)
- Antivirus software installed, including version, and latest updates
- Location of the system(s) involved in the incident (e.g., Washington DC, Los Angeles, CA)
- Method used to identify the incident (e.g., IDS, audit log analysis, system administrator)
- Impact to agency
- Resolution

It is recommended that all incident response teams should utilize this schema when reporting incidents to the US-CERT. Depending upon the criticality of an incident; it is not always feasible to gather all the information prior to reporting it. In this case, incident response teams should continue to report information as it is collected.

Federal Agency Incident Categories

In order to clearly communicate incidents and events (any observable occurrence in a network or system) throughout the Federal Government and supported organizations, it is necessary for the government incident response teams to adopt a common set of terms and relationships between those terms. All elements of the federal government should use a common taxonomy. Below please find a high level set of concepts and descriptions to enable improved communications among and between agencies. The taxonomy below does not replace discipline (technical, operational, intelligence) that needs to occur to defend federal agency computers/networks, but provides a common platform to execute the US-CERT mission. US-CERT and the federal civilian agencies are to utilize the following incident and event categories and reporting timeframe criteria as the federal agency reporting taxonomy.

FEDERAL AGENCY INCIDENT CATEGORIES

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

**Defined by NIST Special Publication 800-61*

DETERMINING THE TYPE OF CYBER-INCIDENT

Computer crime encompasses a broad range of potentially illegal activities. Generally, however, it may be divided into one of two types of categories:

1) Crimes that target computer networks or devices directly; and

2) Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

Table 3 shown on the following page discusses the various types of cyber attacks that an organization may encounter. The GAO analysis of data from government and industry reports[13] accumulated and compiled this data over the last decade, so it should be no surprise to security experts and managers. Regardless of which of the two categories a cyber-attack falls under, the organization must deal with the incident properly. How the organization deals with it is a very large contributing factor into how much that incident will cost in the long run. Studies show a strong correlation between markets for cybercrime and security – as crime increases, so does the market for security mitigation[14] and "without any specific policy intervention, the interaction between the two markets may resemble an arms race.[15]" This fact alone makes it very difficult for insurers to calculate the level of risk and tests organizations resolve to steel themselves against the ever-growing barrage of cyber attacks.

Non-malicious in nature

If the event is not malicious in nature, this incident becomes a scrubbing exercise. Scrubbing each machine of the infection, regardless of whether or not it is malicious, requires someone to physically investigate each device and ensure that it is free of the infection. Depending on the nature of the attack, this could take anywhere from a matter of minutes to several hours. For each device, it is important to track the average time that it takes to sanitize it and put it back online. In an organization that may support thousands of desktop devices, this is not a trivial matter and may require several teams to accomplish the task. To compound the matter, in large corporations this situation may be replicated across multiple locations, further adding to the overall cost of solving this problem. To put this in perspective, consider an organization with 5,000 desktop users, all infected with a virus. Assuming the CSIRT has recognized the problem and isolated the outbreak to the main campus where the 5,000 desktops are situated, it will require 1.5 hours of effort for each user desktop to be cleaned, rebooted and re-scanned. In other words, 5,000 desktops * 1.5 hours * 51.02 burdened cost per hour = $382,650.00 for scrubbing. This should make managers eager to pay a license fee for a good Antivirus protection solution.

[13] GAO-07-705 and GAO, Technology Assessment: Cybersecurity for Critical Infrastructure Protection, GAO-04-321 (Washington, D.C.: May 28, 2004).
[14] Michel J.G. van Eeten and Johannes M. Bauer, "ECONOMICS OF MALWARE: SECURITY DECISIONS, INCENTIVES AND EXTERNALITIES", STI WORKING PAPER 2008/1 (29 May 2008), Information and Communication Technologies JT03246705, Directorate for Science, Technology and Industry, OECD, Paris, France, pp 18.
[15] Ibid.

Types of Cyberattacks	Description
Caller ID Spoofing	A type of attack where the attacker initiates calls with falsified Caller-ID information making it appear to the called party as someone they are not.
Check Sync Reboot	A type of attack where the attacker spoofs or floods "CHECK SYNC" reboot messages into the signaling channel resulting in the caller's phone to constantly reboot.
Denial of Service (DoS)	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed Denial of Service (DD0S)	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Eavesdropping	Unauthorized interception of VoIP IP based calls either before encryption occurs or by analyzer probe of sniffer if unencrypted via malware.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Flooding	A type of Denial of Service (DoS) attack designed to bring a network down by flooding the network with incomplete connection requests, preventing it from processing legitimate traffic.
Fuzzing	Also known as fuzz testing, this is black box software that uses malformed or semi-malformed data injection looking for bugs and vulnerabilities in code.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Man-In-The-Middle (MITM)	Man-in-the-middle, bucket-brigade, or Janus attack occurs is a form of eavesdropping in which the attacker places themselves between proxies and takes over control of the conversation and can impersonate other users.
Phishing	The creation and use of e-mails and web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Redirection	A type of attack where the attacker sends 301/302 moved messages to inbound calls which are then redirected to any phone chosen by the attacker.
Registration Hijacking	A type of attack where the legitimate endpoint registration is replaced with an endpoint pointed to a malicious device rather than the legitimate device.
RTP/Audio Injection	A type of attack where the attacker injects new media or audio into an active media channel.
Session Tear Down	A type of attack where the attacker spoofs or floods "BYE" or "HANGUP" tear down messages into the signaling channel.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwittingly) to propagate.
Vishing	A method of phishing based on voice-over-Internet Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
VoIP SPAM (SPIT)	Spam over Internet Telephony (SPIT) is a type of attack where businesses and individuals are inundated with annoying and resource-draining calls.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.

Table 3 - Understanding various types of cyber attacks.

Malicious in nature

If the event is malicious in nature or of an unknown type, the CSIRT should attempt to classify it. If this is the case, it is almost a certainty that more time will be involved than the organization really wants to spend dealing with a cyber event. Unfortunately, there is really little choice in the matter. If an organization decides to respond inappropriately, usually the impact of such a decision will have devastating and long lasting effects. It is because of this reason many organizations feel like they are held hostage until the effects of such an event can be mitigated. They rely on the expertise and skill of their CSIRTs to resolve the issue, hoping those people have the skills necessary to make quick work of the problem. Unfortunately, this is not the case for many organizations. Studies have shown that organizations not investing in the skill sets necessary to respond to such events until it is too late rarely escape unscathed. A recent study[16] of network administrators showed that *"Nearly four-in-ten (39%) were kept up at night worrying about a security breach to their network in 2010, which was significantly higher than in 2009 (27%). Similar proportions (each year) were kept up at night worrying about their users."* It really becomes a case of "pay me now" or "pay me later." The all too frequent reality is that the "pay me later" part comes sooner than anyone expects.

DETERMINE SOURCE OF CYBER-INCIDENT

It is important to keep vigilant at all times and to have mechanisms to detect a potential compromise or attack via operational practices. When a cyber event occurs, it is important to determine if the event is internal or external in origin. The CSIRT will want to quickly find out if the attack is coming through the firewall or from within its boundaries. In many instances, new cyber incidents can be caused when an unsuspecting user downloads an infected file or installs something they downloaded on their machine, or when they insert a diskette or a flash drive into their machine and that turns out to be infected. Regardless of whether or not the pain is self-inflicted, an organization must still factor in the time and effort expended at this step as a direct labor cost. Once again, consider the effects of this situation in an organization that has thousands of users across dozens of locations. Even if it only takes one day to clean up such a mess, the direct costs as well as the indirect costs, in terms of lost productivity, can add up to very significant numbers quickly.

[16] 7th Annual Survey: Network and System Administrators, Commissioned study conducted by Amplitude Research, Inc., April 30, 2010 by VanDyke Software®, Albuquerque, NM.

The sad reality about cyber attacks is that those targets whom hackers feel are most worth pursuing are most often the largest companies in the world. Attacking a smaller insignificant organization is very much like picking on a little guy just because you're bigger-there is no glory to be had in the matter. Cyber attackers generally go after big fish because it gives them huge bragging rights within their underground communities. Anything less is seen as amateurish and looked down upon within their own community of hacker peers.

Identification

Sometimes the initial notification of an incident may be via phone call or email. Regardless of mechanism of identification, the reported issue should lead to the point of differentiating between an event and an incident. An event is anything that happens in an environment and an incident occurs when that event threatens or causes some harm to the organization. In some events, an incident response team is called because someone sees an event and treats it as suspicious in nature. It is very important to conduct due diligence by reviewing the logs or any other form of evidence to come to a conclusion whether to treat the issue as an event or a potential incident.

Determine if the Threat Will Spread

Once someone has detected that a cyber attack is underway, the organization must quickly determine if it is attempting to propagate. It is important to know if the malware threat is malicious and is attempting to propagate, or even if it is not malicious but still attempting to propagate because the effects can be devastating. If the malware is attempting to propagate, one of the first things the responder must do is isolate the effects of propagation from the network to prevent it from spreading everywhere within the boundaries of the network. This requires quick thinking, quick action, and knowledge that is generally obtained from being well trained and prepared to handle such incidents. The investment in getting someone trained to this level can be considered a preventative cost but, once the event has manifested itself, the actions taken by the CSIRT are absolutely considered as direct costs. In the 2010 survey

mentioned on the previous page[17], when discussing security management issues, threat of virus infections in an organization ranked among the top three concerns.

Marshal the CSIRT

When the incident is reported, the incident handler should document as much as possible in an effort to discern any leading information that could direct the investigation. Once the malicious activity is confirmed, detailed note taking of the handler's actions and chain of custody should be maintained from this point forward. And once it has been confirmed that the events are the result of security incident, the appropriate members of the Incident handling team should be contacted and the official incident management activity be initiated[18].

The act of notifying anyone of a security incident sets off a chain of events, generally cascading into a series of meetings by various departments within the organization to discuss how to resolve the cyber security incident and what the impacts of that incident will be to their specific departments and to the organization as a whole. All of the costs of these meetings should be figured as direct costs of labor. This process requires that participants periodically review the need to convene meetings with the CSIRT.

In many cases, the security response team is busy responding to the event and cannot participate in such meetings. Generally the manager of that team will be the only participant and will provide periodic updates as to the status of the incident. Because of the ripple effect the status updates have with the remaining departments within the organization, it is important that the CSIRT manager provide accurate and timely status. Preparation for and participation in these meetings should also be considered as direct costs.

[17] Unknown, "The Financial Management of Cyber Risk: An Implementation Framework for CFOs", Report published in 2010, the Internet Security Alliance, pp 40.
[18] Northcutt, S (Ed.). Computer Security Incident Handling Step By Step, Version 1.5., SANS Institute, 1998.

Perform Analysis

When a cyber event occurs, it is important for the response team to analyze all available data sources. In order to accurately understand what has happened when a security event occurs, security response teams must look at both internal data and external data, along with any data that is collected proactively during the course of the event. The time taken to collect and analyze this data should be tracked as a direct cost of the event itself. It is important to consider the fact that those who collected data may not be the same people that analyze the data. As an example, the network administrator would gather event logs and send them to a security analyst for review. Just because the response team does not immediately have the data in their possession, it does not mean that those costs of data collection should be overlooked. The person who performs cost accounting for the incident needs to be aware of the amount of effort expended by whom, whenever data collection occurs. It is important to factor in both the source of the data and the cost of obtaining it along with the cost of analyzing that data.

Analyze Internal and External Resources

Internal data generally takes the form of event logs from applications and devices. More often than not, this data will be gathered by asking systems administrators to pull logs from servers within the domains that have been affected by the cyber security incident. Those logs may come from several other sources as well, as discussed in the following sections.

i. **Security Device logs.** Firewalls and routers create logs when events take place. Sometimes logging activities have to be enabled before data can be collected. If the devices are not enabled when an event occurs, there will be no data to review. The adage “an ounce of prevention is worth a pound of cure” holds true in this case.

ii. **Bandwidth Utilization Reports.** Tools used to monitor the network can generally track the utilization of bandwidth and, when spikes in usage occur, alerts and notifications can be made. If there are no such tools in place, then this step cannot occur. The cost of these tools, when used before an incident, would be preventative costs. If they are implemented after an incident, they should be considered remediation costs.

iii. **Network traffic flow data**. In order to monitor traffic flow on a network, a monitoring tool has to be in place. Although the tool itself may be hardware or software, it generally requires someone with the skills necessary to understand what they're doing to use the tool correctly. Once again, consider whether or not this is a preventative or remediated cost, based on the pre or post incident scenario described above.

iv. **Application and system logs**. Application and system logs are used extensively in operating systems and provide a great deal of information. The main drawback the application and system logs is that they create an overwhelming amount of information that must be processed. Generally the processing requires a tool to filter the number of events down to something manageable. Another factor to consider is that many people do not know where all of these logs exist in an operating system environment because they seldom use them. Thus it takes additional time to hunt them down which slows the process of mitigating an event and costs the organization even more money.

In all of the situations described above, each step that takes place is a form of direct labor cost. What is not tracked accurately in most cases is how much time and effort is expended at each of these steps. Careful analysis at this stage will reveal a more accurate picture of the true costs of an incident. Once again, the individual performing cost accounting for the cyber security incident needs to consider both the cost of obtaining the data as well as the cost of analyzing the data.

Over the course of the last decade, with so many cyber security incidents that have taken place, many security staff learned that the quickest way to understand a problem is to simply go out to the Internet and check to see if someone else has dealt with the problem in the past. There are many, many sites that one can check to learn about security events. Regardless of which sites you check or how many of them you check, the act of investigating these sites itself is still a direct labor cost that should be factored in to the overall cost of the incident. The good news here is that in many cases, checking these external sites as a point of reference can often save the organization a great deal of time and money because someone else will have already faced the situation and found a solution to the problem. Being able to leverage someone else's knowledge--particularly if that knowledge has been vetted by reliable source, such as a Federal Agency or well known security organization--will save an organization a great deal of money. Other places to look for external data include:

i. **NIPC/CERT**. The National Infrastructure Protection Center and the Computer Emergency Response Team are both reputable and definitive sources of information for cyber security events. Both of these organizations should be checked before looking elsewhere. Once again, the time it takes to look for an event here should be tracked, but investing time here before going anywhere else will almost always save the organization money in the long run.

ii. **Security Discussion Sites**. There are many security sites out on the Internet that are used to discuss the latest threats to an organization. One of the problems organizations face is in knowing which sites are reputable and can be trusted and which cannot. In addition to this problem, they could also check hacker sites to find out who is bragging about the latest security incidents that have hit the net. Fame and notoriety are strong motivators in the hacker community and that fact should not be underestimated by any security professional.

iii. **Service Provider's Security Team**. In many organizations, particularly very large organizations, it is common practice to outsource Security Services. Because of the high level of skill needed for security teams, it makes sense in many business models to outsource this service as opposed to growing its capability from within an organization.

Due to the unique nature of the cybersecurity domain, it is recommended that incident response skills be developed within the organization for a multitude of reasons, not the least of which is the ability to respond within the least amount of time and for that response to be the correct response every time.

Collecting "Live" Cyber-incident Data

Instances of proactively collected data include all forms of data that, during the course of a security incident, are collected by a CSIRT who possess the skill sets necessary to perform these tasks and the desire to track and prosecute the perpetrators. Because the ripple effects into the customer base of a telecommunications provider can have devastating impact, they are often very eager to work with law enforcement teams to catch cyber attackers. Costs of these data collection activities should be attributed as direct labor costs. Some of the activities these

organizations are willing to support actually do help in the process of gathering information which can be used by the greater telecommunications community to mitigate the effects of future cyber attacks. In this case, "an ounce of prevention is worth a pound of cure." If feasible, it is recommended that these teams examine hostile code collected from:

a. "**Honey pots**" – a honey pot is like a baited trap. It is a network zone specifically designed to lure unauthorized perpetrators into the zone. These perpetrators are looking to gather information that can be used for a variety of purposes. Often the honey pot is filled with bogus data that has very real names and would be seen as attractive targets to attackers. For example, the data could include the latest plans for the next telecommunications widget or the secret codes to the company safe, etc.

b. **Compromised System** - an evaluation of a compromised system can be very time consuming but can also yield a great deal of information. Generally, this is a forensics exercise that requires a very high skill set which equates to a great expense to the organization. This process is described in more detail later in this document. Often, malware and root kits are discovered in this process and these discoveries will lead to an examination of other devices within the compromised network to ensure that this system is not one of many but the only one affected. Costs at this stage are direct labor costs for the individual or individuals performing the forensics work. They can quickly become quite substantial in the case of a propagating event.

c. **Trusted external sources** – sometimes organizations that don't have the capabilities that many telecommunications organizations have will send compromised hosts to an external source for evaluation. Generally this is not a free exercise and the costs can be significant. All of these costs should be reflected as consequential because the organization did not incur them directly but through the services of an outside party.

Sharing Cyber-incident Knowledge

We recommend that organizations that endure the pain of a cyber security incident consider making any collected code and analysis data available to the security community at large. While this, in and of itself, is a very good thing, it still requires internal staff to take the time and effort to notify various organizations and agencies of their findings. Once again, this is a direct cost and should be factored as such. Sometimes, a legal review of the data is required before release and this could be a possible consequential cost as well.

RESPONDING TO THE CYBER-INCIDENT

The primary thing an organization must do when confronted with a cyber security attack is to respond to the attack. Generally, that response will be to marshal troops and point them towards the problem. While it may not seem like this is an obvious cost, the direct cost of labor to perform this additional exercise has to be factored in as part of the overall cost of a cyber security incident. One of the first steps these troops will be tasked to do is to isolate the compromised device from the rest of the network.

Isolate the compromised hosts(s)

Once identification of a compromised device has been made, it can be isolated from the remainder of the network in a variety of ways. This process is sometimes referred to as containment. The core motive of the containment phase is to prevent further damage to any asset impacted by the incident (i.e., data, network, systems, etc.) so the situation does not get any worse. If possible, the first and foremost step in this phase is to remove the impacted system from the network. The most simple and expedient method is simply to disconnect the network connection and take the box offline. When conducting an exercise of this type, it is often common practice to continue this activity over a period of days or even weeks to gather as much information as they can from the attacking party. All of the time spent at this stage is factored into the cost of a cyber security incident as a direct labor cost.

Block Malicious Traffic

When and wherever possible, block malicious traffic with existing security devices; in many instances, such as when a denial of service attack occurs, an organization will try to block malicious traffic to mitigate the extent of damage the attack can cause. Generally some type of network filtering will be applied at this step to prevent traffic from a given source or of a certain protocol from traversing the network. A firewall or perimeter access lists should also be applied in order to prevent any connectivity into or out of the system. In case of a DOS or DDOS attack, the traffic should be directed away from the infected system. And once the damage has been stopped, a detailed analysis of the source/infected system is performed. It is always good to make two copies of the image of the system which is to be analyzed. In order to preserve the evidence, the image of the entire system or part of the system is imaged. Then volatile data is captured, such as all of the running processes.

Once again direct labor costs are the primary factor to consider for calculating the cost of a cyber security incident. Indirectly, the blockage of legitimate traffic also incurs a cost and the calculation of that is highly dependent on the nature of the traffic being blocked. Consider the difference between a brokerage firm executing trades (time sensitive) versus browsing in informational sites such as Wikipedia. The effects are dramatically different and the costs to the organization vary just as greatly.

Mitigate the Event

Where available, apply expedient mitigation techniques (based on analysis of code) – it is commonplace for organizations to try and mitigate the effects of an attack as quickly as they can. In some instances, an analysis of traffic coming into the network needs to happen before a decision can be made as to what action should be taken. Often in these cases, law enforcement agencies are also involved. There are certain times and circumstances where an organization may wish to perform an exercise called backtracking. In this case, the machine most likely would be left online and monitored while cyber security experts analyze the traffic and determine the source of the cyber attack.

In the majority of cases, however, when the incident has been contained, the next step in the process is to remove the infection or remnants of the compromise. It requires complete removal of the malicious code or any data left by the intruder. The compromised system may require a total rebuild from a clean gold image. The important thing to remember before rebuilding a system is to ensure that the back-up systems are free from any infection. After the systems have been restored, the vulnerability analysis of the systems should also be done to ensure the successful eradication of the infection which also confirms no new vulnerabilities are introduced. All intended security controls (i.e., access control lists, host filters, firewall rules, user access permissions, etc.) should be validated to be working properly. Analysis of code or analysis of packets is a time consuming event that requires highly skilled security teams or network staff to accomplish it correctly. In either case, the organization is still facing a direct labor cost that is more than a nominal cost.

Institute Prevention

When possible, patch and harden servers and related networking devices to address specific issues being exploited – this step is seen as a preventative measure and requires time before an attack occurs in order for it to be effective. Time spent patching and hardening systems is time well spent. Cost at this step would be factored into the cost of preventative measures rather than considered a mitigating cost unless those steps were taken after an event. In that case, those costs are the result of remediation and are consequential in nature.

Monitor

One of the necessary steps taken in the recovery process is to monitor both the affected host and the network for signs of subsequent compromise or exploitation. Monitor the network for signs of additional compromise – Vigilance is the cornerstone of success in a network protection scheme. Monitoring, like patching, is considered a preventative measure. One might make the assumption that the approach needed is to add layer upon layer of defenses onto a security protection scheme; that would be a correct one to make. This approach has been referred to by the Department of Defense as a defense in depth strategy[19]. In this approach to protecting data, the basic premise of building up, layering on and overlapping of

[19] Joint Pub 3-13, 9 October 1998, "Joint Doctrine for Information Operations", http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail, the assumption is there are other defensive measures in place that continue to provide protection. These steps are yet another example of the costs of vigilance which we have stated above should be factored in as a preventative cost.

Make Notifications

Where appropriate, the organization should advise vendors and their customers of mitigation/recovery options. This step becomes a bit tricky since the organization that has suffered the attack may not incur direct costs **at this point**. However, the vendor may incur costs related to notification of their customers, actions taken by vendor staff to mitigate the impact of the cyber attack, and even consequential costs that may be attributed to the attack should be factored into the overall cost. There is not a specific methodology for calculating these types of costs, but a common method would be for the organization to inquire of their vendors how many people were used in the process of notification and mitigation as it relates specifically to the event. The vendor organization most likely will translate those costs into direct labor costs which should be tallied from the organization's perspective as a consequential cost simply because the money used to pay for that cost originated from the vendor's coffers and was passed on to the organization after the incident.

Involve Law Enforcement when Necessary

If suspected criminal acts have occurred, report those to your local law enforcement agency. If the cyber incident merits reporting to a law enforcement agency, there will be both direct costs of gathering information to be used as evidence, maintaining a chain of custody for that evidence, and documenting all of the steps taken up to the point when law enforcement takes control of the situation. Conversely, what steps does an organization take to prevent law enforcement agencies from taking action against them if there is a loss of data or a cyber incident? What if they are an international company? The risks can be substantial.

Determine Need for Forensics

During the recovery process, it is important that an organization consider the need to collect data for forensic analysis. In evaluating the magnitude and the severity of a cyber event, the security team often has to make the determination as to whether or not to begin collecting forensic evidence. Generally, if law enforcement needs to be involved, there is a need for forensics. This decision can result in a substantially increased cost to the organization for the incident. Additionally, once the decision has been made to collect forensic evidence, the chain of custody for that evidence must be established in accordance with state and federal guidelines. The general process used for performing digital forensics comprises the following basic phases.[20]

- **Collection**: identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.

- **Examination**: forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.

- **Analysis**: analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

- **Reporting**: reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls) and providing recommendations for improvement to policies, procedures, tools and other aspects of the forensic process.

It is not hard to imagine how quickly these additional costs can add up once this decision has been made. It is for this reason that many organizations simply decide to endure the pain of the cyber incident and forgo any hope of investigation that could lead to an ultimate prosecution of the attacker. Because this decision is made more often than not, the costs here

[20]NIST Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response", NIST, August 2006, pp 9. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html.

should certainly be weighed heavily into the overall cost of the cyber security incident. What many people fail to recognize at this step is the impact of not proceeding with a forensic evidence collection process and incurring the cost of that process. This inaction may actually be more harmful to the organization in the long run. While the organization may save money in direct labor costs, by making such a decision, they need to consider whether that savings actually is greater than the consequential costs they incur by avoiding the evidence collection process.

BEGIN RECOVERY

In the recovery phase, the desire is to return an organization to the state it operated in prior to the cyber attack. Before this can happen, generally there is a lot of work that has already occurred to clean infected hosts and prepare them to go back online. Most organizations will recover compromised hosts in accordance with their disaster recovery or business continuity and disaster recovery plans. In large organizations, it is commonplace to have a disaster recovery and business continuity planning officer. This person would be involved at this stage, along with any appropriate staff, in helping to determine a proper course of action to take in order to recover from the cyber event. Upon validation of the security and business functions, the systems should be put back online. In this phase, QA teams and business partners should be involved to validate the fact that system recovery is successful to make sure that all business processes and functions are back to normal. The final step in the recovery phase is to ensure that the system is being monitored to ensure that future problems are detected in a timely fashion and to look for any additional signs of attack[21].

Next, the CSIRT should survey the infrastructure for other vulnerable hosts and patch/harden systems as appropriate. This step should be considered as a remediation measure and the costs incurred here would be tallied as preventative costs. At this stage, the organization will usually begin to quantify any loss, especially if they seeking legal remedies. The quantification process itself varies greatly from organization to organization but regardless of the organization, it really bears down to either an indirect, direct or consequential cost. The real exercise here is determining at which step to apply which type of cost. Every organization has a finance group that can help them figure out which methods are to be used as they uniquely suit that

[21] Computer Security Incident Response Team, Retrieved July 23, 2010 from http://www.opfro.org/index.html?Components/Producers/Teams/ComputerSecurityIncidentResponseTeam.html~Contents

organization's needs. What is important here is an agreement to align the costs along those three areas so that "apples-to-apples" comparisons can be made when another cyber incident occurs. If other organizations use a similar methodology, then costs between organizations can be compared.

Conduct a Post-mortem

It is not uncommon for an organization to also conduct post-mortem analysis of the cyber security incident and the costs here are direct labor costs because they require time and effort for people to attend meetings and discuss the issues. The importance of this activity is to enhance and improve the incident-handling process and to work through all identified residual issues, discovered during the incident, that improve the security posture of the organization. In this phase the handler should ask the following:

- What systems were compromised?
- How did the compromise occur?
- What steps were taken to contain the incident?
- What steps were taken to clean the infection?
- What steps were taken to ensure the compromise is not repeated again?
- Determine if this is a reportable incident.

All findings should be formally documented with recommendations to be reviewed with stakeholders. The stakeholders must develop action plans with target dates to remediate or minimize the impact of any compromise which occurred. Actions taken as a result of these meetings may translate into preventative costs since they are designed, by their very nature, to avoid a repeat of the incident. Often organizations will revise procedures and conduct training based on post-mortem analysis. Any change an organization makes as a result of a cyber security incident, in order to prevent a reoccurrence of the effects of that incident, should be construed as a preventative measure. As such, the costs should be considered preventative.

At this stage, the organization will usually begin to formally quantify any loss, especially if they seeking legal remedies. The quantification process itself varies greatly from organization to organization but, regardless of the organization, it really is either an indirect, direct or consequential cost. The real exercise here is determining at which step to apply which type of cost. Every organization has a finance group that can help them figure out which methods are

to be used as they uniquely suit that organization's needs. What is important here is an agreement to align the costs along those three areas so that "apples-to-apples" comparisons can be made when another cyber incident occurs. If other organizations use a similar methodology, then costs between organizations can be compared.

Finally, in the recovery stage, organizations often look towards their legal department for review of actions taken from the time notification of the incident occurred until a walk into the legal office to discuss it. Generally, the legal team will want a chronological summation of all activities taken throughout the course of the cyber security incident. Once again, this will require someone to expend the effort needed to create these documents. These direct costs are almost always overlooked and should not be since they can also add up to a significant amount of work and money. The framework of thought presented in this document should help companies find a path forward when an incident takes place. More importantly, it should help them mitigate the effects of an incident by having the knowledge to prepare before an incident occurs and to minimize the effects (costs) to the maximum extent possible.

INCIDENT RESPONSE MATURITY

One aspect of Incident response that is often overlooked is Incident Response (IR) Maturity. This view of IR analyzes the character of the IR strategy implemented by the organization. Just as there is a difference in the maturity of people, ranging from a baby, a child, a teenager, young adult, middle-aged and senior citizen, there can also be differences in the maturity and capability of an organization's IR approach. When we describe an individual, we rarely stop at "he's human." So why should we limit the classification of IR plans to a single group? We understand the maturity concept when applied to people. We know that as a baby grows and becomes a child, his or her abilities change, increase and become more refined. But this child can't do everything that the older individuals can do. Similarly, not all IR strategies are as effective, robust and comprehensive as others.

Once we consider the characteristic of maturity when it comes to Incident Response, we must decide how to measure the difference. How do we grade or classify IR strategies so that a meaningful comparison or evaluation can be made? Additionally, there will likely be different aspects of IR maturity to consider, and an organization may be more mature in one area than

another. A similar concern exists when it comes to understanding the maturity of an organization's security. The Information Systems Auditability and Control Association (ISACA) developed the COBIT[22] framework to help organizations understand its security and audit requirements within its technology department. One component to COBIT is the concept of Maturity Model. COBIT looks at four areas of IT:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

COBIT proposes several controls for each group above to support the organization, but it also applies a maturity model. Six levels of maturity are then used to classify the organization's control environment:

1. Non existent
2. Initial/ad hoc
3. Repeatable but intuitive
4. Defined
5. Managed and Measureable
6. Optimized

We might supply a similar approach to help understand the maturity differences between IR strategies. If we were to group all of the other discussion in this document into four areas, we might focus on:

- Incident Governance
- Incident Planning
- Incident Response
- Incident Analysis

[22] COBIT 4.1 – IT Governance Institute, ISACA. www.isaca.org

For each of these areas we could then apply a multi-level grading system that helps describe how well the organization has adopted the IR strategy. For the sake of this discussion, let us refer to the maturity levels described in COBIT. The following are just general descriptions of these four areas. The reader is urged to go to the specific sections of this document for more detail.

Incident Governance

Incident governance describes the high level strategy and support that comes from the highest levels of the organization and includes:

- Formal statement of support signed by the CEO or Chairman and approved by the board.
- Charter or mission statement for the purpose of planning for, identifying, addressing and analyzing incidents that impact the normal operations of the organization.
- Support for a mechanism to provide the appropriate executive data regarding incidents to the executive team so that appropriate top-level involvement is maintained.
- Functional support in the form of funding, personnel, reporting structure, etc. to deliver on the elements of the IR charter.

Incident Planning

The best time to deal with an incident is before it occurs--in other words through effective planning. Several questions need answers before the first sign of a problem:

- Have you defined what an incident is?
- Have you identified and categorized the assets?
- Have you identified the threats?
- Have you designed and documented an Incident Response Plan?
- Is your Incident Response Plan kept up-to-date?
- Has the relevant personnel been trained for an incident?
- Do you conduct scenario testing?

- Have you included participation and support from legal, PR, operations, regulatory, HR and financial departments within your organization?

Incident Response

How well does the organization address the response to an incident? Is it ad hoc, off-the-cuff or do they have scripted and tested responses that are flexible enough to address the incident as well as detailed enough to speed decision making and response? Does the organization have the personnel with proper training and the right tools to address the incident? Is the response manually initiated or automatic? Each of the suggestions put forth in this document must stand this same test: how well does the organization implement the suggestion? Other questions include:

- What is the scope of monitoring?
- All systems or just "critical" systems?
- Support for 24x7 or 8x5 operations?
- On-site or remote support?
- What data or information is critical and what can be replaced?
- Is there appropriate legal, HR, and technical guidance?
- Are the channels of communication formally opened or only as needed?

Incident Analysis

Even after the incident is resolved the work is not done – the incident and the response must be analyzed.

- Do you know what data has legal significance?
- How do you discover all relevant data for Legal?
- Did you maintain the chain of custody?
- Do you have an established storage retention plan for maintaining chain of custody data?
- Do you have the skill set internally to complete forensic analysis?

- Do you analyze the event to improve response effectiveness in the future?

These topics and questions are just examples of those that need to be considered when determining the maturity of your IR strategy. This aspect of incident response is not to get a "passing grade" or "to do better than the competition." It is meant to assess the strengths and weaknesses within your IR plan. With this knowledge you can, through repeated improvement and reassessment, grow your strategy into a mature and extremely effective solution.

REAL-TIME SITUATIONAL AWARENESS IN CYBERSPACE

We recommend all organizations take steps to improve real-time situational awareness and enhance the identification of network anomalies. Doing so can better protect federal and public cyberspace and national infrastructure. Security incidents from federal agencies are on the rise, increasing by over 400 percent from fiscal years 2006 to 2009.[23] The U.S. Computer Emergency Readiness Team (US-CERT) leads a public - private partnership to protect and defend the nation cyber infrastructure. It coordinates and facilitates information-sharing among federal agencies, state and local government, private sector business entities, academia, international partners, and the general public on cyber security threats and attacks.[24] US-CERT is mandated with sharing cyber security information with the public and private sectors through various working groups, issuing notices, bulletins, and reports, and when postings. US-CERT is hindered in its ability to provide an effective analysis and warning program for the federal government in a number of ways, specifically:

1. US-CERT does not have the appropriate enforcement authority to help mitigate security incidents. It operates by providing analytical insight into cyber activity, creating conduits for technical analysis of data, and by characterizing the threat, vulnerability, and incident response. Additionally, agencies would be required to respond to incidents no later than 24 hours after discovery or provide notice to US-CERT as to why no action has been taken. Finally, agencies would have to ensure that the information security vulnerabilities were mitigated timely.

[23] GAO Testimony before the Committee on Homeland Security, House of Representatives. CYBERSECUIRTY GAO-10-834T

[24] U.S. Department of Homeland Security, Office of the Inspector General, Readiness Assessment of the U.S. Computer Emergency Readiness Team's (US-CERT) June 7, 2010.

2. US-CERT is unable to monitor federal cyber space in real-time and the tools used do not allow for real time analysis of network traffic. As a result US-CERT will continue to be challenged in protecting federal cyber space from security related threats. Currently US-CERT maintains a near-real-time situational awareness as it performs information aggregation activities.
3. US-CERT collects data in real-time but it must also be able to perform analysis on the data in near-real-time. Cyber analysts receive information from a variety of sources and other US-CERT activities are used to identify potential incidents and to assess their possible scope and impact on the nation's cyber infrastructure.
4. US-CERT employs technology systems and tools to fulfill its mission requirements to protect and defend nation's infrastructure against potential threats and cyberspace, and respond to security incidents. Currently US-CERT uses a wide variety of tools to detect and mitigate cyber security incidents.

With the introduction of the Einstein program, US-CERT can gather more network traffic information and identify cyber activity patterns. However, US-CERT cannot capture all network traffic because Einstein has not been deployed to all federal agencies since, in its initial stages, the deployment of Einstein 1 to federal agencies was entirely voluntary. In September 2008, OMB made Einstein part of the trusted Internet connections initiative and required all agencies to install sensors on their networks.[25,26] As of October 2009, they deployed Einstein 1 to 19 agencies and Einstein 2 to eight agencies. Currently, US-CERT is conducting a pilot program to exercise Einstein's capabilities. According to a comprehensive national cyber security initiative and US-CERT officials, Einstein 3 will not contain real time full packet inspection and intrusion prevention features. These additions should give US-CERT better response and monitoring capabilities.

According to US-CERT officials, many agencies have not installed Einstein because they have not consolidated their gateways to the Internet.[27] Some agencies have fragmented networks and must upgrade their architectures before Einstein can be deployed. Additionally, US-CERT does not have an automated correlation tool to identify trends and anomalies. With the vast amounts of network traffic, US-CERT experienced a long lead time to analyze potential security

[25] OMB Memorandum M-08-27, Guidance for Trusted Internet Connection Compliance, September 2008.
[26] OMB Memorandum M-08-05, Implementation of Trusted Internet Connection, November 2007.

[27] U.S. Department of Homeland Security, Office of the Inspector General, Readiness Assessment of the U.S. Computer Emergency Readiness Team's (US-CERT) June 7, 2010.

threats and abnormalities. To reduce the lead-time, an automated correlation tool was purchased to analyze the data from Einstein. However, US-CERT is currently experiencing problems with reconfiguring the tool to collect data and understand the overall data flow. US-CERT management stated that it may be six months before the problems are corrected and the benefits of the system can be seen.

With the Homeland Security Act of 2002, DHS was required to establish appropriate systems, mechanisms and procedures to share homeland security information, relevant to threats and vulnerabilities in national critical infrastructure, with other federal departments and agencies, state and local governments and the private sector, in a timely manner. The National Strategy to Secure Cyberspace recommends that DHS coordinate with other federal agencies to share specific warning information and advise them of appropriate protective measures and counter measures. An effective analysis and warning program is critical to secure the Federal information technology infrastructure and national critical infrastructure. For US-CERT to perform its responsibilities successfully, it must have significant technical resources and analytical tools and technologies to identify, collect, analyze and respond to cyber attacks.

Currently the National Security Agency is launching an expansive program dubbed "Perfect Citizen" to detect cyber assaults on private companies and government agencies running such critical infrastructure as electricity grid and nuclear power plants[28]. Perfect Citizen, in theory, would rely on a set of sensors deployed in computer networks' for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack, though it wouldn't persistently monitor the whole system.

Perfect Citizen Systems will look at large, typical older computer control systems that were often designed without Internet connectivity or security in mind many of those systems which run everything from subway systems to air traffic control networks have been linked to the Internet and making them more efficient but also exposing them to cyber attacks. According to NSA the program is purely a vulnerability assessment and capabilities development contract, a research and engineering effort[5]. By taking into consideration all these efforts to bridge the gap and create a real-time awareness and mitigation program, the FCC would need to create:

[28] Wall Street Journal "U.S. Plans Cyber Shield for Utilities, Companies" 7-8-2010

- Widespread information security control efficiencies.
- Trusted Internet Connections (TIC) between carriers.
- Collaborative working environment with inter agency programs like Perfect Citizen.

Today, cyber-incidents are handled in reactive mode. At best, only ”near real time” can be achieved and even then would only be near real time for isolated incidents. A coordinated multi-tiered cyber-incident could gridlock the system, resources, and ability to analyze and mitigate. A strategy that would provide the capability to respond real time and be proactive in mitigation rather than respond in a reactive mode is sorely needed. Combined with updated security policies and practices to incorporate the aforementioned strategy would ensure successful mitigation across all spectrums of cyber-incidents.

	Wireless (1)	IP Services (2)	Network (3)	People (4)	Legacy Services (5)
	WIFI Bluetooth Mobile Devices Mobile Devices Application Security Emerging Devices Wireless 3G, 4G, Microwave, & Satellite	Broadband Cloud Computing IPV6 Voice over IP	Access Control Availability Confidentiality Integrity Security Mgmt Security Audit & Alarm Security Policy & Standard Recovery Intrusion Detection	Awareness SPAM Social Engineering Data Loss / Data Leakage Phishing Security Policy	Media Gateways Communication Assisted Law Enforcement (CALEA) Signal Control Points (SCP) Gateway to Gateway Protocol SS7
	Rodney Buie Micah Maciejewski Gary Toretti Bill Garret	**Chris Garner** Jim Payne Ray Singh Barry Harp Bill Garret	**John Knies** Doug Peck Rajeev Gopal Ron Mathis Jeremy Smith	**Fred Fletcher** Ramesh Sepehrrad Allison Growney John Coleman	**Robin Howard** Doug Davis Uma Chandrashekhar

Identity Mgmt (6) Idm Lifecycle Access Control Strong Authentication Certificates SAML Policy Password Role Base Access Control Systems Administration	**Martin Dolly** Jim Payne Brian Moir Rajeev Gopal Ray Singh
Encryption (7) Encryption Keys Cellular Networks Device Encryption Voice Encryption Data Encryption Key Management Key Recovery Cloud Standards	**Dan Hurley** Ron Mathis John Rittinghouse Tim Thompson Jim Ransome Anthony Grieco Annie Sokol Bob Thornberry
Vulnerability Mgmt (8) Alerting Risk & Vulnerability Assessment Mitigation Asset Inventory Patch Mgmt	**Micah Maciejewski** John Knies Jermey Smith Fernandez Francisco Rodney Buie
Incident Response (9) Policy & Plan Prevention Attack Detection Response & Mitigation	**John Rittinghouse** Barry Harp Robin Howard Myrna Soto Fred Fletcher

New	**164**
Modified	**161**
Original	**72**
	397

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
New	**Ad-hoc Wifi Policies:** Service Providers and Network Operators should implement policies and practices that prohibit ad-hoc wireless networks. An ad-hoc wireless network is a peer-to-peer style network connecting multiple computers with no core infrastructure. They are not considered secure and are commonly associated with malicious activity.	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf	Wireless / WIFI	Cyber Security; Wireless Access Point;	0	0	1	0	0	0	1	1	0	0	0	1
New	**Wifi Policies:** Service Providers and Network Operators should establish policies to ensure only authorized wireless devices approved by the network managing body or network security are allowed on the network. Unauthorized devices should be strictly forbidden.	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf	Wireless / WIFI	Cyber Security; Wireless Access Point;	0	0	1	0	0	0	1	1	0	0	0	1
New	**Wifi Standards:** Service Providers,and Network Operators, should implement applicable industry standards for wireless authentication, authorization, and encryption (e.g. WPA2 should be considered a minimum over WEP which is no longer considered secure).	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf	Wireless / WIFI	Cyber Security; Wireless Access Point; Wireless Authentication;	0	0	1	0	0	0	1	1	0	0	0	1
New	**Wifi Standards:** Service Providers and Network Operators should implement applicable industry standards to ensure all devices on the Wireless LAN (WLAN) network enforce network security policy requirements.	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf	Wireless / WIFI	Cyber Security; Wireless Access Point; Network Security Policy;	0	0	1	0	0	0	1	1	0	0	0	1
New	**Wifi Intrusion Prevention/Detection:** Network Operators should consider installation of a Wireless Intrusion System at all locations to detect the presence of unauthorized wireless systems. At a minimum, routine audits must be undertaken at all sites to identify unauthorized wireless systems.	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml	Wireless / WIFI	Cyber Security; Wireless Access Point; Wireless Audits;	0	0	1	0	0	0	0	1	0	0	0	2
New	**WiFI Signal Strength:** Service Providers & Network Operators should minimize wireless signal strength exposure outside of needed coverage area.	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf	Wireless / WIFI	Cyber Security; Wireless Access Point;	0	0	1	0	0	0	1	1	0	0	0	3
New	**Blue Tooth Interfaces**: Network Operators should turn off Bluetooth interfaces when not in use and disable Bluetooth's discovery feature, whereby each device announces itself to all nearby devices.	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth;	0	0	1	0	0	0	0	1	0	0	0	3

New	**Blue tooth Power:** Network Operators should configure Bluetooth devices to use the lowest power that meets business needs. Class 3 (encrypts all traffic) devices transmit at 1 mW and cannot communicate beyond 10 meters, while class 1 devices transmit at 100 mW to reach up to 100 meters. For best results, use mode 3 to enforce link authentication and encryption for all Bluetooth traffic, and discourage business use of devices that support only mode 1 (no encryption).	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Bluetooth Passwords:** Network Operators should password protect both devices to prevent use of lost / stolen units. If possible, do not permanently store the pairing PIN code on Bluetooth devices.	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Awareness:** Service Providers and Government should promote education for the safe use of all Bluetooth-capable devices and define security policies that impact business.	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth; Policy	0	0	1	0	0	0	1	0	0	0	1	3
New	**Bluetooth Paring:** Network Operators should pair devices in a private location using a long random PIN code. Avoid default PIN codes, easily guessed PIN codes ("000") and devices that do not support configurable PIN Codes.	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Bluetooth Authentication:** Network Operators should require authentication on both devices. Configure Bluetooth products so that users must accept incoming connection requests.	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Bluetooth Scanning:** Network Operators and Government should scan the airwaves (where possible) inside your business to locate all Bluetooth capable devices. Inventory all discovered devices with Bluetooth interfaces, including hardware model, OS, and version. Perform searches on Bluetooth vulnerability and exposure databases to determine whether the devices are impacts.	http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html	Wireless / Bluetooth	Cyber Security; Wireless; Blue Tooth;	0	0	1	0	0	0	0	1	0	0	1	3
New	**Awareness:** Service providers should educate their Enterprise customers on the importance of establishing a mobile device security policy to reduce threats without overly restricting usability.	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets	0	0	1	0	0	0	1	0	0	0	0	3
New	**Mobility Handset Passwords:** Service Providers and Network Operators should enforce strong passwords for mobile device access and network access. Automatically lock out access to the mobile device after a predetermined number of incorrect passwords (typically five or more).	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Passwords;	0	0	1	0	0	0	1	1	0	0	0	2

New	**Mobility Handset Wipe:** Service Providers and Network Operators should perform a remote wipe (i.e. reset the device back to factory defaults) when an employee mobile device is lost, stolen, sold, or sent to a third party for repair. Organizations need to have a procedure set for users who have lost their devices	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	1	1	0	0	0	2
New	**Mobility Handset Encryption:** Network Operators should encrypt local storage (where possible), including internal and external memory.	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobility Handset VPN:** Network Operators should enforce the use of virtual private network (VPN) connections between the employee mobile device and enterprise servers.	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobiity Handset Upgrades**: Network Operators should perform centralized configuration and software upgrades "over the air" rather than relying on the user to connect the device to a laptop / PC for local synchronization.	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobility Handset Security**: Network Operators should ensure that mobile applications remove all enterprise information from the device.	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobility Handeset Security Education:** Service Providers and Network Operators should provide a program of employee education that teaches employees about mobile device threats and enterprise mobile device management and security policies.	http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	1	1	0	0	0	3
New	**Mobility Handset Applications**: Network Operators should limit the installation of unsigned third party applications to prevent outside parties from requisitioning control of your devices.	http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobility Handset Firewalls:** Network Operators, where possible, should setup unique firewall policies specifically for traffic coming from smart phones.	http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobility Handset Intrusion Detection:** Network Operators, where possible, should have intrusion prevention software examine traffic coming through mobile devices.	http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3

New	**Mobility Handset Antivirus:** Network Operators, where possible, should utilize anti-virus software for the mobile devices.	http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/	Wireless / Mobile Device	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	0	1	0	0	0	3
New	**Femtocell Security:** Service Providers and Network Operators should ensure connections between Femtocell and Femto Gateway follow industry standardized IPSec protocol. Connection between Femtocell and Femto OAM system must be based on TLS/SSL protocol while management traffic flow is outside of the IPSec tunnel. Optionally, the management traffic may also be transported through Secure Gateway over IPSec once the IPSec tunnel between Femtocell and Secure Gateway is established.		Wireless / Emerging Devices /Femtocell	Cyber Security; Wireless; Femtocell;	0	0	1	0	0	0	1	1	0	0	0	2
New	**Femtocell Security:** Service Providors should ensure that enterprise Femtocell Hardware authentication must be certificate based.		Wireless / Emerging Devices /Femtocell	Cyber Security; Wireless; Femtocell; Security;	0	0	1	0	0	0	1	0	0	0	0	2
New	**Femtocell Security:** Equipment Suppliers should ensure enterprise Femtocell hardware shall be tamper-proof.		Wireless / Emerging Devices /Femtocell	Cyber Security; Wireless; Femtocell; Security;	0	0	1	0	0	0	0	0	1	0	0	3
New	**Femtocell Security:** Service Providers should ensure all security relevant events, e.g. apparent security violations, completion status of operations, invalid or unsuccessful logon attempts, userid, logon time, etc are to be recorded.		Wireless / Emerging Devices /Femtocell	Cyber Security; Wireless; Femtocell; Security;	0	0	1	0	0	0	1	0	0	0	0	3
New	**Wireless Equipment Patching:** Equipment Suppliers and Service Providers should have processes in place to ensure that all third party software (e.g. operating system) have been properly patched with the latest security patches and that the system works correctly with those patches installed.		Wireless / Emerging Devices /Femtocell	Cyber Security; Wireless; Femtocell; Security;	0	0	1	0	0	0	1	0	1	0	0	3
New	**Femtocell Security:** Service Providers and Network Operators should ensure Femtocell access control is flexible to be based on: individual Femtocell; or group of Femtocells; and/or entire Enterprise Femto System. The access control list administration, where feasible should be web GUI based, and userid / password authenticated.		Wireless / Emerging Devices /Femtocell	Cyber Security; Wireless; Femtocell; Security;	0	0	1	0	0	0	1	1	0	0	0	3
New	**Wireless Encryption:** Service Providers and Equipment Suppliers should establish application support for cryptography that are based on open and widely reviewed and implemented encryption algorithms and protocols. Examples of acceptable algorithms and protocols include AES, Blowfish, RSA, RC5, IDEA, SSH2, SSLv3, TLSv1, and IPSEC. Products should not rely on proprietary or obscure cryptographic measures for security.		Wireless / Mobile Device / Application Baselines Cryptography	Cyber Security; Mobile Handsets;	0	0	1	0	0	0	1	0	1	0	0	3

New	**Wireless Encryption:** Equipment Suppliers in order to secure all key exchange applications, algorithms with strengths similar to 2,048-bit RSA or Diffie-Hillman algorithms with a prime group of 2,048 bits should be used. Anonymous Diffie-Hillman must not be supported.		Wireless / Mobile Device / Application Baselines Cryptography	Cyber Security; Mobile Handsets;	0	0	1	0	0	0	0	0	1	0	0	3
New	**Wireless Policies and Standards:** Service Providers, Network Operators, and Equipment Suppliers should design passwords used for an application login to be consistent with applicable industry security guidelines and policies. Whether between the client and the server or among servers, passwords must not be transmitted "in the clear." SSL should be used for any transaction involving authentication. The transmission of session IDs should be similarly protected with SSL.		Wireless / Mobile Device / Application Baselines Cryptography	Cyber Security; Mobile Handsets; Passwords;	0	0	1	0	0	0	1	1	1	0	0	3
New	**Wireless Encryption:** Service Providers and Network Operators should implement for all symmetric secure data integrity applications, algorithms with strengths similar to HMAC-MD5-96 with 128-bit keys, HMAC-SHA-1-96 with 160-bit keys, or AES-based randomized message authentication code (RMAC) being the standard used.		Wireless / Mobile Device / Application Baselines Cryptography	Cyber Security; Mobile Handsets;	0	0	1	0	0	0	1	1	0	0	0	3
New	**Wireless Encryption:** Service Providers and Network Operators should implement Authenticated Key Agreement (AKA) protocol to provide user and network with a session specific random shared-key that can be used for confidential communication.		Wireless / Cellular / 3G	Cyber Security; Cellular network;	0	0	1	0	0	0	1	1	0	0	0	2
New	**Protection from eavesdropping:** Service Providers and Network operators should take steps to protect user data from evasdropping and/or being tampered in transit; Ensure user has the correct credentials; Accuracy and efficiency of accounting.		Wireless / Cellular / 4G	Cyber Security; Cellular network;	0	0	1	0	0	0	1	1	0	0	0	2
New	**Wireless Encryption:** Service Providers and Network Operators should take steps to ensure all traffic on a 4G network is encrypted using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which uses AES for transmission security and data integrity authentication.		Wireless / Cellular / 4G	Cyber Security; 4G network;	0	0	1	0	0	0	1	1	0	0	0	2
New	**Wireless Encryption:** Service Providers and Network Operators should enable the Mobile MiMAX system to provide secure communications by encrypting data traffic and use PKM (Privacy Key Management) Protocol that allows for the Base Station to authenticate the MS/CPE and not vice versa.		Wireless / Cellular / 4G	Cyber Security; 4G network;	0	0	1	0	0	0	1	1	0	0	0	3

New	**Wireless Authentication:** Service Providers and Network Operators should use strong certificate-based authentication ensuring network access, digital content and software services can be secured from unauthorized access.		Wireless / Cellular / 3G / 4G	Cyber Security; Cellular network;	0	0	1	0	0	0	1	1	0	0	0	3
New	**Wireless Encryption:** Service Providers, Network Operators, and Equipment Suppliers should use NSA approved encryption and authentication for all Satcom command uplinks; downlink data encrypted as applicable depending on sensitivity/classification.	Committee on National Security Systems Policy (CNSSP) 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, 20 March 2007	Wireless / Microwave & Satellite	Cyber Security; Satellite	0	0	0	1	0	0	1	1	1	0	0	2
New	**Mitigation Strategies:** Service Providers and Network Operators should implement mitigation strategies against physical threat vectors that affect the satellite, the availability of communications, the integrity and confidentiality of satellite, and the performance of communications.	"Satellite Security" Online Journal of Space Communication, number 6 (Winter 2004) http://spacejournal.ohio.edu/issue6/main.html	Wireless / Microwave & Satellite	Cyber Security; Satellite	0	0	0	1	0	0	1	1	0	0	0	3
New	**Wireless Standards:** Service Providers and Network Operators should consider integration of open standardized protocols to meet communication-level performance and security goals.	Space Communications Protocol Standards (SCPS) Including ISO Standards 15891:2000 through 15894:2000 and related documents http://www.scps.org/	Wireless / Microwave & Satellite	Cyber Security; Satellite	0	0	0	1	0	0	1	1	0	0	0	3
NRIC 7-7-8106 Unchanged	**Wireless Standards:** Network Operators, Service Providers and Equipment Suppliers should employ operating system hardening and up-to-date security patches for all accessible wireless servers and wireless clients. Employ strong end user authentication for wireless IP connections. Employ logging of all wireless IP connections to ensure traceability back to end user. In particular, vulnerable network and personal data in cellular clients must be protected if the handset is stolen. Apply good IP hygiene principles.		Wireless / Device & Server Vulnerabiity Prevention	Cyber Security; Wireless	0	0	1	0	0	0	1	1	1	0	0	3
New	**Mobility Handset Standards:** Network Operators should sanitize employee mobile devices when removed from service. Mobile devices and other electronic equipment that contain or access sensitive information, or have been used to access sensitive information in the past, should be processed to ensure all data is permanently removed in a manner that prevents recovery before they are disposed of as surplus equipment or returned to the vendor.	Source: http://www.k-state.edu/its/security/procedures/mobile.html	Wireless /Data Loss-Leakage / Awareness	Cyber Security; Wireless Handsets	0	0	1	0	0	0	0	1	0	0	0	3
New	**Mobility Handset Standards:** Network Operators should required Data Encryption for all employee mobile devices that contain sensitive data. If sensitive information must reside on a mobile device, it should be encrypted. The decryption key should be entered manually; this step should not be automated. A means should exist to recover encrypted data when the decryption key is lost. Require the use of laptop encryption and **password-protection**.	Source: http://www.k-state.edu/its/security/procedures/mobile.html	Wireless / Data Encryption	Cyber Security; Wireless Handsets	0	0	1	0	0	0	0	1	0	0	0	3

New	**Mobility Handset Standards:** Network Operators should set policy that requires any sensitive information transmitted to or from the employee mobile device be encrypted and/or transferred with a secure data transfer utility. Use of a secure connection or protocol, such as SSL, that guarantees end-to-end encryption of all data sent or received should be included in policy. Devices with wireless capability pose an additional risk of unauthorized access and tampering. These capabilities should be disabled, secured, or protected with a firewall.	Source: http://www.k-state.edu/its/security/procedures/mobile.html	Wireless / Data Loss-Leakage / Data Transmission	Cyber Security; Wireless Handsets	0	0	1	0	0	0	0	1	0	0	0	3
NRIC 7-7-8104 Unchanged	**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.		Wireless LAN / Access Control	Cyber Security; Wireless Access Point;	0	0	1	0	0	0	1	1	0	0	0	3
NRIC 7-7-8058 Changed	**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.	Wireless / Access Control	Cyber Security; Cellular network;	0	0	1	0	0	0	1	1	0	0	0	3
NRIC 7-6-8060 Changed	**Protect Against Cellular Network Denial of Service:** Service Providers & 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.	Wireless / Availability	Cyber Security; Cellular network;	0	0	1	0	0	0	1	1	0	0	0	3

NRIC 7-7-8106 Changed	**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.	Telcordia GR-815.	Wireless / System Hardening and Patching	Cyber Security; Cellular network;	0	0	1	0	0	0	1	1	1	0	0	2
New	**Wireless Tethering:** Service providers should devise a means of enforcing security over tethered connections. When Tethering via a mobile device for data communication, an encryption methodology, such as IPSEC or SSL/VPN should be utilized to ensure session security.	http://en.wikipedia.org/wiki/Tethering	Wireless / Tethering	Cyber Security; Wireless Handsets; Security;	0	0	1	0	0	0	1	0	0	0	0	3

New	**47**
Modified	**3**
Original	**2**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7 6-6-0806 Changed	**Service Policies:** Service Providers should establish policies and develop internal controls to ensure that the infrastructure supporting high speed broadband is protected from external threats, insider threats and threats from customers. These policies should cover protocol and port filtering as well as general security best practices.		IP Services / Broadband	Cyber Security; Network Operations; Broadband	1	1	0	0	1	0	1	0	0	0	0	1
NRIC 7 6-6-0807 Changed	**Service Policies:** Service Providers should establish policies and develop internal controls to ensure that individual users have availability, integrity, and confidentiality and are protected from external threats, insider threats and threats from other customers. These policies should cover protocol and port filtering as well as general security best practices.		IP Services / Broadband	Cyber Security; Network Operations; Broadband	1	1	0	0	1	0	1	0	0	0	0	1
NRIC 7 6-6-0813 Changed	**Service Awareness:** Service Providers should encourage users to take steps to maintain the availability, integrity and confidentiality of their systems and to protect their systems from unauthorized access. Service Providers should enable customers to get the tools and expertise to secure their systems.		IP Services / Broadband	Cyber Security; Network Operations; Broadband	1	1	0	0	1	0	1	0	0	0	0	1
NRIC 7 7-P-0814 Unchanged	**Service Reliability:** For the deployment of Residential Internet Access Service, Broadband Network Operators should design in the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance, security, or usage policy.		IP Services / Broadband	Cyber Security; Network Operations; Broadband	1	1	0	0	1	0	0	1	0	0	0	1
NRIC 7 7-P-0822 Unchanged	**Service Policies:** For the deployment of Residential Internet Access Service, a Broadband Network Operator should incorporate multilevel security schemes for network data integrity and availability, as applicable, in the network design to prevent user traffic from interfering with network operations, administration, and management use.		IP Services / Broadband	Cyber Security; Network Operations; Broadband	1	1	0	0	1	0	0	1	0	0	0	2
New	**Service Standards:** Service Providers should develop and implement security event logging systems and procedures to allow for collection of security related events.		IP Services / Broadband	Cyber Security; Network Operations; Broadband	1	1	0	0	1	0	1	0	0	0	0	3
New	**General:** Service Providers and Network Operators [that provide or manage Customer Premise Equipment (CPE)] should ensure that initial configurations are secure.		IP Services / Broadband	Cyber Security; Network Operations; Broadband;	1	1	0	0	1	0	1	1	0	0	0	3

New	**General:** Service Providers should classify their cloud service against one of the defined industry cloud service architecture models (e.g., software as a service [SaaS], platform as a service [PaaS] or infrastructure as a service [IaaS]) and the deployment model being utilized (e.g., private cloud, community cloud, public cloud or hybrid cloud) to determine the general "security" posture of the specific cloud service, how it relates to asset's assurance and security protection requirements, and define the needed security architecture to mitigate security risks.	NIST 800-53 revision 3: Recommended Security Controls for Federal Information Systems and Organizations security control catalogue. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1	IP Services / Cloud Computing	Cyber Security; Network Operations; Cloud Security;	1	1	0	0	1	0	1	0	0	0	0	3
New	**Risk Management and Governance in the Cloud:** Service Providers should periodically conduct risk assessments of their information security governance structure and processes, security controls, information security management processes, and operational processes.	NIST 800-53 revision 3: Recommended Security Controls for Federal Information Systems and Organizations security control catalogue. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1	IP Services / Cloud Computing	Cyber Security; Network Operations; Cloud Security;	1	1	0	0	1	0	1	0	0	0	0	3
New	**Cloud Business Continuity Planning and Disaster Recovery:** Service Provider should have a documented Business Continuity and Disaster Recovery Plan.	NIST 800-53 revision 3: Recommended Security Controls for Federal Information Systems and Organizations security control catalogue. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1	IP Services / Cloud Computing	Cyber Security; Network Operations; Cloud Security; Disaster Recovery, Emergency Preparedness	1	1	0	0	1	0	1	0	0	0	0	2
New	**General:** Service Provider and Network Operators should implement access controls (firewalls, access control lists, etc.) to administrative interfaces as well as those normally carrying customer traffic.	IETF RFC 4942	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	2
New	**General:** Service Providers and Network Operators should test current equipment for IPv4/IPv6 compatibility for the specific network deployment.	NIST SP 800-119 (Draft) 2.4	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	2
New	**Routing Integrity:** Service Providers and Network Operators should use explicit static configuration of addresses, routing protocols and parameters at peering point interfaces rather than neighbor discovery or defaults.		IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Routing Integrity:** Service Providers and Netwrok Operators should employ protocol-specific mechanisms or IPSec as applicable	NIST SP 800-119 (Draft) 3.6.2	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Routing Integrity:** Service Provider and Network Operators should use static neighbor entries rather than neighbor discovery for critical systems		IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3

New	**Routing Integrity:** Service Provider and Network Operators should use BGP ingress and egress prefix filtering, TCP MD5 or SHA-1 authentication	NIST SP 800-54	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Routing Integrity:** Service Providers and Network Operators should use IPv6 BOGON lists to filter un-assigned address blocks at Network boundaries.		IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Packet Filtering:** Service Providers and Network Operators should apply IPv6 and IPv4 anti-spoofing and firewall rules as applicable, wherever tunnel endpoints decapsulate packets.	NIST SP 800-119 (Draft) 6.5.2	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Packet Filtering:** Service Providers and Network Operators should have access control lists for IPv6 that are comparable to those for IPv4, and that also block new IPv6 multicast addresses that ought not to cross the administrative boundary.	NIST SP 800-119 (Draft) 4.2.3	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Packet Filtering:** Service Providers and Network Operators should block tunneling protocols (for example, IP protocol 41 and UDP port 3544) at points where they should not be used. Tunnels can bypass firewall/perimeter security. Use static tunnels where the need for tunneling is known in advance.	NIST SP 800-119 (Draft) 2.4	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	1	1	0	0	1	0	1	1	0	0	0	3
New	**Packet Filtering:** Service Providers and Network Operators should filter internal-use IPv6 addresses at provider edge and network perimeter.	IETF RFC 4942 2.1.3	IP Services / IPV6	Cyber Security; Network Design; Network Operation, Network Interoperability; IPV6	0	0	1	0	1	0	1	0	0	0	0	3
New	**VOIP Standards:** Service Providers and Network Operators should use dedicated VoIP servers for the VOIP service, if possible	DISA - VoIP0270	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	3
New	**Packet Filtering:** Service Providers and Network Operators should block protocols meant for internal VoIP call control use at the VoIP perimeter.	DISA-VoIP0220 DISA-VoIP0230	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	3
New	**Packet Filtering:** Service Providers and Network Operators should proxy remote HTTP access to the VoIP perimeter firewalls.	DISA-VoIP0245	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	3

New	**Administration:** Service Providers and Network Operators should block VoIP firewall administrative/management traffic at the perimeter or Tunnel/encrypt this traffic using VPN technology or administer/manage this traffic out of band	DISA-VoIP0210	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	3
NRIC 7-6-8055 Changed	**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.	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	3
NRIC 7-7-8535 Changed	**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.	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	1
NRIC 7-7-8056 Changed	**Operational Voice over IP (VoIP) Server Hardening:** Network Operators should ensure that network servers have authentication, integrity, and authorization controls in place in order to prevent inappropriate use of the servers. Enable logging to detect inappropriate use.	NSA (VOIP and IP Telephony Security Configuration Guides), and PacketCable Security 2.0 Technical Report (PKT-TR-SEC-V05-080425).	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	0	1	0	0	0	3
NRIC 7-6-8057 Changed	**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, general, control, and management.	NSA (VOIP and IP Telephony Security Configuration Guides), and PacketCable Security 2.0 Technical Report (PKT-TR-SEC-V05-080425).	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	0	0	1	0	0	3
New	**VOIP Standards:** Service Providers and Network Operators should route HTTP access from the VoIP environment through the data environment and use HTTPS if at all possible.	DISA-VoIP0245	IP Services / VoIP	Cyber Security; Network Design; Network Operation, Voice over IP (VoIP)	1	1	0	0	0	0	1	1	0	0	0	3
New	**21**															

Modified	**7**
Original	**2**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7-7-8112 Changed	**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.		Network / Access Control / 3rd party access and levels	Cyber Security; Network Operations; Access Control	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8086 Unchanged	**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.	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	Network / Access Control / Access request authorization	Cyber Security; Network Operations; Access Control	0	0	0	0	1	0	1	1	1	0	0	2
NRIC 7-7-8115 Changed	**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		Network / Access Control / Controlling access to operating system software	Cyber Security; Network Operations; hardware; Access Control	0	0	0	0	1	0	0	0	1	0	0	1

NRIC 7-7-8022 Changed	**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.		Network / Access Control / Controlling remote user access	Cyber Security; Network Operations; Access Control, Remote Access;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8521 Unchanged	**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.		Network / Access Control / Controlling remote user access	Cyber Security; Network Operations; Access Control; VPN	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8018 Changed	**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/ - 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	Access Control/Managing access control standards (Intranet, Extranet, Internet)	Cyber Security; Network Operations; Access Control; Hardening	0	0	0	0	1	0	1	1	1	0	0	1
NRIC 7-7-8091 Unchanged	**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. Periodic, applications-specific flushing of the cache should also occur.		Network / Access Control /Managing access control standards (Intranet, Extranet, Internet)	Cyber Security; Network Operations; Access Control;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-8102 Unchanged	**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.		Network / Access Control / Managing access control standards (Intranet, Extranet, Internet)	Cyber Security; Network Operations; Policy; Desktop; Access Control	0	0	0	0	1	0	1	1	1	0	0	3

NRIC 7-7-8006 Changed	**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	Network / Access Control / Managing network access controls	Cyber Security; Network Operations; Access Control;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8040 Changed	**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.		Network / Access Control / Managing network access controls	Cyber Security; Network Operations; Netwrok Design; Access Control	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-6-8093 Unchanged	**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	Network / Access Control / Managing network access controls	Cyber Security; Network Operations; Network Interoperability	0	0	0	0	1	0	1	0	0	0	0	1
NRIC 7-7-8135 Changed	**Protection of Devices Beyond Scope of Control:** Equipment Suppliers should implement techniques such as tamper-proof cryptochips/authentication credentials and authentication for (service provider) configuration controls, in customer premises equipment.	PacketCableTM Security Specification PKT-SP-SEC-I11-040730, IETF RFC 3261	Network / Access Control / Managing network access controls	Cyber Security; Network Operation; Access Control;	0	0	0	0	1	0	0	0	1	0	0	3

NRIC 7-6-8012 Changed	**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/ - 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 ITU - CCITT Rec. X.700 (X.720) Series ITU - CCITT Rec. X.800 Series ITU-T Rec. X.805 ITU-T Rec. X.812	Network / Access Control / Managing network access controls	Cyber Security; Network Operation, Access Control	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8024 Changed	**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/ - ATIS-0300276.2008 Operations,	Network / Access Control / Managing user access	Cyber Security; Network Operation; Access Control	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8030 Unchanged	**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.		Network / Access Control / Managing user access	Cyber Security; Network Operation; Access Control;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8083 Unchanged	**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, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 69-124.	Network / Access Control /Managing user access	Cyber Security; Network Operation; Access Control; Emergency Preparedness	0	0	0	0	1	0	1	1	1	0	0	3

NRIC 7-6-8087 Changed	**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.		Network / Access Control / Managing user access	Cyber Security; Network Operation; Access Control;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8098 Changed	**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.	Network / Access Control / Managing user access	Cyber Security; Network Operation,; Access Control;	0	0	0	0	1	0	1	1	1	0	0	1
NRIC 7-7-8522 Changed	**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.		Network / Access Control / Managing user access	Cyber Security; Network Operation; Network Elements; Access Control	0	0	0	0	1	0	1	1	0	0	0	3

NRIC 7-7-8565 Unchanged	**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.		Network / Access Control / Managing user access	Cyber Security; Network Operation; Access Control	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-8078 Unchanged	**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.	Network / Access Control / Password	Cyber Security; Network Operation; Access Control	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8507 Changed	**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	Network / Access Control/Role based access control	Cyber Security; Network Operation; Access Control;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-6-8096 Changed	**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).	Network / Access Control / User rights and responsibilities	Cyber Security; Network Operation; Access Control; Security Systems	0	0	0	0	1	0	1	1	0	0	0	2

NRIC 7-7-0507 Changed	**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).	"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	Network / Availability / Attack Detection, Prevention, and Mitigation	Cyber Security; Network Operation; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	1	0	0	2
NRIC 7-7-8134 Changed	**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.		Network / Availability / Change Control	Cyber Security; Network Operation; Security Systems; Access Control; Network Elements	0	0	0	0	1	0	1	0	0	0	0	3
NRIC 7-7-8003 Changed	**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.		Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Design; Network Operation; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8005 Changed	**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	Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Design; Network Operation; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	3

NRIC 7-7-8095 Changed	**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.	Additional resources are required to provide prioritized transport even when overloaded.	Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Design; Network Operation; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8117 Changed	**DNS Servers Disaster Recovery Plan:** Service Providers and Network Operators should prepare a disaster recovery plan to implement upon DNS server compromise.	Disaster recovery plan may need to address backup DNS strategy (addressed by 7-7-8527)	Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Operation; Disaster Recovery	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8131 Unchanged	**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.		Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Operation; Business Continuity	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8132 Changed	**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.		Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Operation; Business Continuity;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8133 Changed	**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.		Network / Availability / Continuity of Operations (COOP)	Cyber Security; Network Operation; Business Continuity; Disaster Recovery	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-6-8047 Changed	**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)	Network / Availability / Specfic Attacks – Denial of Service etc.	Cyber Security; Network Operation; Network Design; Network Elements	0	0	0	0	1	0	1	1	0	0	0	2

NRIC 7-6-8048 Changed	**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)	Network / Availability / Specfic Attacks – Denial of Service etc.	Cyber Security; Network Operation; Network Design; Network Elements	0	0	0	0	1	0	1	1	1	0	0	2
NRIC 7-6-8049 Changed	**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.	Network / Availability / Specfic Attacks – Denial of Service etc.	Cyber Security; Network Operation; Network Design; Network Elements	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8089 Unchanged	**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	Network Confidentiality/Information Classification	Cyber Security; Network Design; Network Elements	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-8017 Changed	**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/ - 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	Network / Confidentiality / Secure protocols	Cyber Security; Network Design; Network Elements; Network Provisioning	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8114 Changed	**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.		Network / Confidentiality / Secure protocols	Cyber Security; Network Design; Network Elements; Network Operations	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8116 Changed	**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)	Network / Confidentiality / Secure protocols	Cyber Security; Network Design; Network Elements; Network Operations	0	0	0	0	1	0	1	1	1	0	0	3

NRIC 7-7-8128 Changed	**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.		Network / Security Audit and Alarm/Managing reports	Cyber Security; Network Design; Network Elements; Network Operations	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-8069 Changed	**Monitoring Requests:** Service Providers and Network Operators 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.		Network / Security Audit and Alarm / Monitoring 3rd party services	Cyber Security; Network Design; Network Elements; Network Operations	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8127 Changed	**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.		Network / Security Audit and Alarm / Monitoring operational audit logs	Cyber Security; Network Design; Network Elements; Network Operations	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8088 Changed	**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.	Information Security Forum. "Security Audit/Review". The Forum's Standard of Good Practice, The Standard for Information Security. **November 2000.**	Network / Security Audit and Alarm /Monitoring system and network access	Cyber Security; Network Design; Network Elements; Network Operations	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-8038 Unchanged	**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.		Network / Security Audit and Alarm / Systematic evaluation of the system and network security	Cyber Security; Network Design; Network Elements; Network Operations; Policy	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8121 Unchanged	**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/	Network / Security Audit and Alarm / Systematic evaluation of the system and network security	Cyber Security; Network Design; Network Elements; Network Operations; Policy	0	0	0	0	1	0	1	1	1	0	0	3
New	**Use continuity management to protect information:** Service Providers and Network Operators should establish a business continuity process for information, identify the events that can classified as business interuption, test and update the business continuity plan.	ISO 27002 Information Security Standards	Network / Security Management / Backup and recovery procedures	Cyber Security; Network Operation; Business Continuity	0	0	0	0	1	0	1	1	0	0	0	3

NRIC 7-7-8042 Changed	**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. NIST SP 800-54 Border Gateway Protocol Security	Network / Security Management / Controlling shared networks	Cyber Security; Network Design; Network Elements; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	1
New	**Network Connection Control:** Service Providers and Network Operators should ensure that access to shared networks, including those that cross organizational boundaries, as well as internal network and customer management infrastructures, is restricted, as per the Company's access control policy. These restrictions apply to systems, applications, and users, and is enforced via a router, firewall,or similar device allowing for rule-based traffic filtering, thereby ensuring a logical separation of networks.	ISO/IEC 27002 (17799) [2005]	Network / Security Management / Controlling Shared Networks	Cyber Security; Network Design; Network Elements; Network Operations; Security Systems	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8063 Changed	**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.	NIST SP800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf	Network / Security Management/IPS/IDS	Cyber Security; Network Design; Network Elements; Network Operations; Security Systems	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8072 Changed	**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.	NIST SP800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf	Network / Security Management/IPS/IDS	Cyber Security; Network Operation; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8073 Changed	**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.	NIST SP800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf	Network / Security Management/IPS/IDS	Cyber Security; Network Operation; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	1
New	**Protect exchange of information:** Service Providers, Network Operators, and Equipment Suppliers should consider establishing information exchange policies and procedures, establish information and software exchange agreements, safeguard transportation of physical media.	ISO 27002 Information Security Standards	Network / Security Management/Managing onsite and remote data stores	Cyber Security; Network Design; Network Operations; Policy;	0	0	0	0	1	0	1	1	1	0	0	3

NRIC 7-6-8101 Changed	**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.	NIST SP800-14 Generally accepted principles and practices for securing IT systems. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf	Network / Security Management/Managing system documentation	Cyber Security; Network Design; Network Operations; Documentation;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-6-8041 Changed	**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.		Network / Security Management/Network Configuration and management	Cyber Security; Network Design; Network Operations; Network Elements;	0	0	0	0	1	0	0	0	1	0	0	3
NRIC 7-6-8043 Changed	**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 unauthorized route injection (particularly from compromised customers) by egress filtering (to peers) and ingress filtering (from customers) prefixes set to other ISPs, 6) Stop DoS from 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 NIST SP 800-54 Border Gateway Protocol Security	Network /Security Management/Network Configuration and management	Cyber Security; Network Design; Network Operations; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-6-8044 Changed	**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).	Network / Security Management/Network Configuration and management	Cyber Security; Network Design; Network Operations; Network Elements; Network Interoperability;	0	0	0	0	1	0	1	1	0	0	0	3

NRIC 7-7-8046 Changed	**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" NIST SP 800-81 & SP 800-81 R1 Secure Domain Name System(DNS) Deployment Guide	Network / Security Management/Network Configuration and management	Cyber Security; Network Design; Network Operations; Network Elements; Network Interoperability; Physical Security management;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-6-8050 Changed	**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 NIST SP 800-54 Border Gateway Protocol Security ITU - CCITT Rec. X.800 Series (X.811 & X.812)	Network / Security Management/Network Configuration and management	Cyber Security; Network Design; Network Operations; Network Elements; Network Interoperability; Physical Security management;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-6-8090 Changed	**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.	ITU-T Rec. X.815 (?? ISO/IEC 8073) Rec. ITU-T X.1031	Network / Security Management/Network Configuration and management	Cyber Security; Network Design; Network Operations; Network Elements;	0	0	0	0	1	0	1	1	1	0	0	2
NRIC 7-7-8008 Changed	**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 ITU-T Rec. X.805 ITU-T Rec. X.812	Network / Security Management/Network Segregation	Cyber Security; Network Design; Network Operations; Network Elements; Security Systems;	0	0	0	0	1	0	1	1	1	0	0	1

NRIC 7-6-8015 Changed	**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/ - 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 ITU-T X.805	Network / Security Management/Network Segregation	Cyber Security; Network Design; Network Operations; Network Elements; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8025 Changed	**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	Network / Security Management/Network Segregation	Cyber Security; Network Design; Network Operations; Network Elements; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8509 Changed	**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 ITU-T Rec. X.1051	Network / Security Management/Network Segregation	Cyber Security; Network Design; Network Operations; Network Elements; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8108 Changed	**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. In addition, it is important to have a means of alternate authenticated access to a system in the event of a failure. In the case of core routers failing CLOSED, there should be a secondary means of authentication (e.g., use of a one-time password) reserved for use only in such an event; this password should be protected and only accessible to a small key-contingent of personnel	ITU-T Rec. X.1051	Network / Security Management/Responding to system faults	Cyber Security; Network Operations; Network Elements; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	1

NRIC 7-7-8136 Changed	**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 ITU-T Rec. X.1051	Network / Security Management/Responding to system faults	Cyber Security; Network Design; Network Operations; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8531 Changed	**Recover from MPLS (Multi-Protocol Label Switching) Misconfiguration:** 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	Netowrk / Security Management/Routing Controls	Cyber Security; Network Design; Network Operations; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-6-8045 Changed	**Protect Interior Routing Tables:** Service Providers and 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.	http://www.ietf.org/rfc/rfc1321.txt	Network / Security Management/Routing Controls	Cyber Security; Network Design; Network Operations; Network Elements; Network Interoperability	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8525 Changed	**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	Network / Security Management/Routing Controls	Cyber Security; Network Design; Network Operations; Network Elements; Network Interoperability	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8526 Unchanged	**Recover from Interior Routing Table Corruption:** If the interior routing has been corrupted, Service Providers and Network Operators should implement policies that filter routes imported into the routing table. The same filtering methods used in NRIC 8045 can be applied more aggressively. The malicious routes will expire from the table, be replaced by legitimate updates, or in emergencies, can be manually deleted from the tables. If needed, the authentication mechanism/crypto keys between IGP neighbors should also be changed.		Network / Security Management/Routing Controls	Cyber Security; Network Design; Network Operations; Network Elements; Network Interoperability	0	0	0	0	1	0	1	1	0	0	0	1

New	**Protect Unattended Workstations:** Service Providers and Network Operators should have policies and enforce that unattended workstations should be protected from unathorized access 1) Individual Username/Password authentication must be required to access resources. 2) Physical access must be restricted to workstations. 3) Where possible idle workstations must default to password protected screensaver after an established time lapse (e.g. 15 minutes).	http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf Octave Catalog of Practices, Version 2.0, CMU/SEI-2001-TR-20 (http://www.cert.org/archive/pdf/01tr020.pdf) Practice OP1.2.4	Network / Security Management/Securing unattended workstations	Cyber Security; Network Operations; Policy; Desktop; Access Control;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8007 Changed	**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.	NIST Special Publication 800-53, Revision 3, Control Number PM-7 Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf NIST Special Pub 800-12, NIST Special Pub 800-14	Network / Security Management/Security Architecture	Cyber Security; Network Operations; Network Design; Policy; Business Continuity;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-6-8016 Changed	**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/ - 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	Network / Security Management/Security Architecture	Cyber Security; Network Operations; Network Design; Policy; Business Continuity; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8506 Changed	**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.	Network / Security Management/Security Architecture	Cyber Security; Network Operations; Network Design; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8508 Changed	**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,	Network / Security Management/Security Architecture	Cyber Security; Network Operations; Network Design; Network Procedures; Policy; Disaster Recovery; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	3

NRIC 7-7-8000 Changed	**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 compensating controls, such as proxy servers, firewalls, or router filter lists, if such services are required for a business purpose.	Configuration guides for security from NIST (800-53 Rev. 3), NSA (Security Configuration Guides), and Center For Internet Security (CIS Benchmarks).	Network / Security Management/System Hardening and Patching	Cyber Security; Network Operations; Network Design; Network Elements; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8004 Changed	**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.		Network / Security Management/System Hardening and Patching	Cyber Security; Network Operations; Network Design; Network Elements;	0	0	0	0	1	0	0	0	1	0	0	3
NRIC 7-6-8010 Changed	**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/ - 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	Network / Security Management/System Hardening and Patching	Cyber Security; Network Operations; Network Design; Network Elements;	0	0	0	0	1	0	0	0	1	0	0	3
NRIC 7-6-8011 Changed	**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/ - 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	Network / Security Management/System Hardening and Patching	Cyber Security; Network Operations; Network Design; Network Elements;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8019 Changed	**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 (800-53 Rev. 3), NSA (Security Configuration Guides), Center For Internet Security (CIS Benchmarks) '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	Network / Security Management/System Hardening and Patching	Cyber Security; Network Operations; Network Design; Network Elements;	0	0	0	0	1	0	1	1	1	0	0	1

NRIC 7-7-8123 Unchanged	**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.		Network / Security Policy and Standards/Governance	Cyber Security; Network Operations; Network Design; Network Elements; Policy	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8097 Changed	**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, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 555-592 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.	Network / Security Policy and Standards/Information life cycle management	Cyber Security; Policy	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-8066 Changed	**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.		Network / Security Policy and Standards/Sharing information with 3rd parties	Cyber Security; Industry Cooperation;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-6-0811 Changed	**Specified Rate Services:** 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.		Network / Security Policy and Standards/Sharing information with 3rd parties	Cyber Security; Network Operations; Network Design;	0	0	0	0	1	0	1	0	0	0	0	3

NRIC 7-7-0808 Changed	**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	Network / Security Policy and Standards/Sharing information with 3rd parties	Cyber Security; Network Operations; Network Design;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8033 Changed	**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/ - 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 Common Criteria: http://www.iso.org, http://csrc.nist.gov/cc/; Carnegie-Mellon Software Engineering Institute secure software development:	Network / Security Policy and Standards/Software development life cycle	Cyber Security; Policy; Software; Application Security;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8113 Unchanged	**Network Standard:** Network Operators, Service Providers and Equipment Suppliers should not permit local logon of users other than the system administrator. Local logon of a system administrator should be used only as a last resort.		Network / Login Security	Cyber Security; Network Operations; Access Control; Procedures	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8139 Unchanged	**Network Standard:** Network Operators and Service Providers should review and analyze security-related event data produced by critical systems on a regular basis to identify potential security risks and issues. Automated tools and scripts can aid in this analysis process and significantly reduce the level of effort required to perform this review.		Network / Security-Related Data Analysis	Cyber Security; Network Operations; Policy; Procedures	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8507 Unchanged	**Incident Response:** When it is discovered that a system is running with a higher level of privilege than necessary, Network Operators and Service Providers should consider which systems/services the affected system could be disconnected from to minimize access and connectivity while allowing desired activities to continue; conduct a forensic analysis to assess the possibility of having potentially compromised data and identify what may have been compromised and for how long it has been in a compromised state; and reconnect system to back-office with appropriate security levels implemented.		Network / Recovery	Cyber Security; Network Operations; Procedures; Forensics; Incident Response;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-0449 Unchanged	**SPAM:** Network Operators and Service providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.		Network / SPAM Controls	Cyber Security; Network Operations; Network Design; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-0515 Unchanged	**Abuse Communications:** Network Operators and Service Providers should, for easy communication with subscribers and other operators and providers, use of specific role-based accounts (e.g., abuse@provider.net, ip-request@provider.net) versus general accounts (e.g., noc@provider.net) which will help improve organizational response time and also reduce the impact of Spam.		Network / Role-Based Mailbox	Cyber Security; Network Operations; Network Design; Security Systems; Access Control;	0	0	0	0	1	0	1	1	0	0	0	3

NRIC 7-7-0547 Unchanged	**Database Security:** Network Operators and Service Providers should place critical network databases (e.g., directory server, feature server, Service Control Point (SCP)) in a secure environment across distributed locations to provide service assurance (e.g., maintainability, connectivity, security, reliability) consistent with other critical network elements.		Network / Secure Environments	Cyber Security; Network Operations; Network Design; Physcial Security Management	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8083 Unchanged	**Database Security:** Network Operators, Service Providers and Equipment Suppliers who use authentication databases/files should: -Protect these databases / files from unauthorized access, -Back-up and securely store these databases / files 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.		Network / Protect Authentication Files and/or Databases	Cyber Security; Network Operations; Business Continuity; Network Design; Security Systems;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8024 Unchanged	**Operations Security:** Network Operators, Service Providers and Equipment Suppliers should not permit users to log on locally to the Operation Support Systems or network elements. System administrator console logon should require as strong authentication as practical.		Network / Limited Console Access	Cyber Security; Network Operations; Access Control;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8046 Unchanged	**DNS Security:** Network Operators and Service Providers should protect against DNS server compromise by implementing protection such as physical security, removing all unnecessary platform services, monitoring industry alert channels for vulnerability exposures, scanning DNS platforms for known vulnerabilities and security breaches, implementing intrusion detection on DNS home segments, not running the name server as root user/minimizing privileges where possible, and blocking the file system from being compromised by protecting the named directory.		Network / Domain Name System	Cyber Security; Network Operations; Access Control;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8063 Unchanged	**Intrusion Detection/Prevention:** Network Operators and Service Providers should install and actively monitor IDS/IPS tools. Sensor placement should focus on resources critical to the delivery of service.		Network / Intrusion Detection & Prevention Tools (IDS/IPS)	Cyber Security; Network Operations; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	2

NRIC 7-7-8063 Unchanged	**Intrusion Detection/Prevention:** Network Operators and Service Providers should maintain and update IDS/IPS tools regularly to detect current threats, exploits, and vulnerabilities.		People/Data Loss-Leakage/Intrusion Detection & Prevention Tools (IDS/IPS)	Cyber Security; Network Operations; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8073 Unchanged	**Intrusion Detection/Prevention:** Network Operators and Service Providers should deploy Intrusion Detection/Prevention Tools with an initial policy that reflects the universe of devices and services known to exist on the monitored network. Due to the ever evolving nature of threats, IDS/IPS tools should be tested regularly and tuned to deliver optimum performance and reduce false positives.		People/Data Loss-Leakage/Intrusion Detection & Prevention Tools (IDS/IPS)	Cyber Security; Network Operations; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8064 Unchanged	**Intrusion Detection/Prevention:** Network Operators and Service Providers should generate and collect security-related event data for critical systems (i.e. syslogs, firewall logs, IDS alerts, remote access logs, etc.). Where practical, this data should be transmitted to secure collectors for storage and should be retained in accordance with a data retention policy. A mechanism should be enabled on these systems to ensure accurate timestamps of this data (e.g., Network Time Protocol).		Network / Security-Related Data Collection	Cyber Security; Network Operations; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	2
NRIC 7-7-8111 Unchanged	**Digital Certificates:** Network Operators, Service Providers and Equipment Suppliers, certificates should have a limited period of validity, dependent upon the risk to the system, and the value of the asset. -If there are existing certificates with unlimited validity periods, and it is impractical to replace certificates, consider the addition of passwords that are required to be changed on a periodic basis.		Network / Expiration of Digital Certificates	Cyber Security; Network Operations; Access Control; authentication;	0	0	0	0	1	0	1	1	1	0	0	3
NRIC 7-7-8118 Unchanged	**DNS Distributed Denial of Service:** Network Operators and Service Providers should provide DNS DDoS protection by implementing protection techniques such as: 1) Rate limiting DNS network connections 2) Provide robust DNS capacity in excess of maximum network connection traffic 3) Have traffic anomaly detection and response capability 4) Provide secondary DNS for back-up 5) Deploy Intrusion Prevention System in front of DNS.		Network / Domain Name System	Cyber Security; Network Operations; Security Systems; Intrusion Detection;	0	0	0	0	1	0	1	1	0	0	0	1
NRIC 7-7-8509 Unchanged	**Incident Response:** When, through audit or incident, a co-mingling of data or violation of a trust relationship is discovered, Network Operators and Service Providers should, as part of a post-mortem process, review segmentation design to evaluate adequacy of the architecture and data isolation.		Network / Recovery	Cyber Security; Network Operations; Incident Response;;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators should block incoming email file attachments with specific extensions know to carry infections, or should filter email file attachment based on content properties.	Source: Stopping Spam – Report of the Task Force on Spam – May 2005IS	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	0	1	0	0	0	3

New	**Spam:** Network Operators should establish inbound connection limits on all services.	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations; Network Design	0	0	0	0	1	0	0	1	0	0	0	3
New	**Spam:** Service Providers and Network Operators should stop all access attempts from IP Addresses with no reverse DNS at the connection level.	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators should stop all SMTP traffic that has reverse DNS, which reflects home PC connections (i.e. 0.0.127.mydialup.bigisp.com).	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	0	1	0	0	0	3
New	**Spam:** Network Operators should employ Optical Character Recognition techniques which allow the ability to read text even when it appears as a graphic image.	Source: Anti-Spam Best Practices and Technical Guidelines	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	0	1	0	0	0	3
New	**Spam:** Network Operators should perform content analysis of In-bound e-mails.	Source: Anti-Spam Best Practices and Technical Guidelines	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	0	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should apply URL detection techniques to detect the domain name of spammers.	Source: Anti-Spam Best Practices and Technical Guidelines.	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should avoid acting as a backup MX for other companies.	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators should avoid quarantining email as much as possible.	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	0	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should consider employing IP Reputation Services.	Source: Combating Spam – Best Practices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should enforce SMTP authentication.	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should not allow default catch all addresses.	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should not routinely bounce email wherever possible (valid user checking and virus scanning).	Source: http://www.linuxmagic.com/opensource/anti_spam/bestpractices	Network / PREVENTING SPAM – ISPs and Network Operators	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators should check sender authentication	Source: Anti-Spam Best Practices and Technical Guidelines	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	0	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should employ DNS lookup techniques which are able to determine if the sending e-mail is legitimate and has a valid host name.	Source: Anti-Spam Best Practices and Technical Guidelines	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
New	**Spam:** Network Operators and Service Providers should establish an Internal Email Address to which Spam can be forwarded by Employees.	Source: Anti-Spam Best Practices and Technical Guidelines	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3

New	**Spam:** Network Operators and Service Providers should use Anti-Relay Systems to Protect Mail servers from being hijacked.	Source: Anti-Spam Best Practices and Technical Guidelines	Network / PREVENTING SPAM – END USERS AND ORGANIZATIONS	Cyber Security; Network Operations;	0	0	0	0	1	0	1	1	0	0	0	3
NRIC 7-7-8077 Unchanged	**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.	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	Network / Access Control / Managing access control standards (Intranet, Extranet, Internet)	Cyber Security; Network Operations; Network Design; Access Control;	0	0	0	0	1	0	1	1	0	0	0	2
New	**Network Access Control for Signaling:** Network Operators should ensure that signaling interface points that connect to IP Private and Corporate networks interfaces are well hardened and protected with firewalls that enforce strong authentication policies.		Network / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Operations; Network Design; Security Systems;	0	0	0	0	1	0	0	1	0	0	0	1
New	**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.	Network / Unauthorized Changes	Cyber Security; Network Operations; Network Design; Security Systems;	0	0	0	0	1	0	1	1	0	0	0	3

New	**23**
Modified	**66**
Original	**32**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7-7-5091 Unchanged	**Travel Security Awareness:** Network Operators, Service Providers and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.		People/Awareness/Security Awareness	Cyber Security; Emergency Preparedness; Public Safety;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-5270 Unchanged	**Cybersecurity Awareness:** Network Operators, Service Providers, Equipment Suppliers and Property Managers personnel should be aware that terrorists or malicious groups may use false information to cause heightened public or employee awareness to divert attention and resources to other areas away from their intended physical or cyber target. Where feasible, information (e.g., news sources, e-mail) should be authenticated and cross-verified to ensure accuracy of information.		People/Awareness/Security Awareness	Cyber Security; Emergency Preparedness; Public Safety; Training & Awareness;	1	1	1	1	1	1	1	1	1	1	0	3
New	**Cybersecurity Awareness:** Network Operators, Service Providers and Equipment Suppliers should develop employee education programs that emphasize the need to comply with security policies.	http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/06/15/laptop-encryption-software-for-social-security-administration-telecommuters.aspx	People/Awareness/Security Awareness	Cyber Security; Public Safety; Training & Awareness; Policy	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8070 unchanged	**Cybersecurity Awareness:** Network Operators and Service Providers should have Abuse Policies and processes posted for customers (and others), instructing them where and how to report instances of service abuse. Service Providers, Network Operators, and Equipment Suppliers should support the email IDs listed in rfc 2142 "MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS."		People/Spam/Abuse Reporting	Cyber Security; Public Safety; Training & Awareness;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-7-8097 Unchanged	**Data Leakage:** Network Operators, Service Providers and Equipment Suppliers should create an enforceable policy clearly defining who can disseminate information, and what controls should be in place for the dissemination of such information. The policy should differentiate according to the sensitivity or criticality of the information.		People/Data Loss-Leakage/Information Dissemination	Cyber Security; Data Leakage; Training & Awareness;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8124 Unchanged	**Cybersecurity Awareness:** Network Operators, Service Providers and Equipment Suppliers should ensure staff is given awareness training on security policies, standards, procedures, and general best practices. Awareness training should also cover the threats to the confidentiality, integrity, and availability of data including social engineering. Training as part of new employee orientation should be supplemented with regular refreshers to all staff.	This is an accepted BP	People/Data Loss-Leakage/Awareness Training	Cyber Security; Public Safety; Training & Awareness; Policy;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-7-8125 Unchanged	**Cybersecurity Awareness:** Network Operators, Service Providers and Equipment Suppliers should ensure that employees formally acknowledge their obligation to comply with their corporate Information Security policies.		People/Awareness/Security Awareness	Cyber Security; Public Safety; Training & Awareness; Policy;	1	1	1	1	1	1	1	1	1	0	0	3

NRIC 7-7-5067 Changed	**Cybersecurity Awareness**: Network Operators, Service Providers and Equipment Suppliers should make security an ongoing priority and implement an annual compliance requirement for the completion of a security awareness program.	Source: http://ezinearticles.com/?Employee-Security-Awareness&id=4084497	People/Awareness/Security Awareness	Cyber Security; Public Safety; Training & Awareness; Policy;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8124 Changed	**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. 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.	Source: 2009 Carnegie Mellon University, Author: Mindi McDowell posted on: http://www.us-cert.gov/cas/tips/ST04-014.html	People/Social Engineering	Cyber Security; Training & Awareness; Policy;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8129 Changed	**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.		People/Awareness/ Training and Exercise	Cyber Security; Training & Awareness;	1	1	1	1	1	1	1	1	1	0	0	3
New	**Customer Acceptable Use Policy:** Network Operators and Service Providers should develop an acceptable use policy for customers of their services and enforce it.		People/Awareness/Security Awareness	Cyber Security; Policy;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Cybersecurity Awareness:** Network Operators, Service Providers and Equipment Suppliers should create a security awareness strategy that includes communicating to everyone from new hires to human resources to senior management. Utilize multiple channels and target each audience specifically.	http://www.securityinnovation.com/pdf/security-awareness-best-practices.pdf	People/Awareness/Security Awareness	Cyber Security; Training & Awareness;	1	1	1	1	1	1	1	1	1	0	0	3

New	**Threat Management:** Network Operators, Service Providers and Equipment Suppliers should keep their programs flexible. What is considered a security best practice today might be obsolete tomorrow. Changing factors include new technologies, changing business models, emerging threats and growth of the network and the user base.	http://ezinearticles.com/?Employee-Security-Awareness&id=4084497	People/Awareness/Security Awareness	Cyber Security; Training & Awareness; Threats;	1	1	1	1	1	1	1	1	1	0	0	3
New	**Management Support:** Network Operators, Service Providers and Equipment Suppliers should obtain senior management approval and support for a corporate wide People/Awareness/Security Awareness program. This will help to lead to behavior and policy changes.	http://www.securityinnovation.com/pdf/security-awareness-best-practices.pdf	People/Awareness/Security Awareness	Cyber Security; Training & Awareness;	1	1	1	1	1	1	1	1	1	0	0	3
New	**Employment:** Network Operators, Service Providers and Equipment Suppliers should work with their HR departments to consider making acknowledgement and agreement regarding information security a condition of employment.	http://ezinearticles.com/?Employee-Security-Awareness&id=4084497	People/Awareness/Security Awareness	Cyber Security; Training & Awareness; Human Resources;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Social Engineering Vulnerability Assessment:** Network Operators and Service Providers should consider conducting Social Engineering Audits such as tests for vulnerabilities or unauthorized access to systems, networks and information. Systems range from computer networks to physical access to locations.	Sources : http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Sharon.htm http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-HackerTactics.html http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Dolan.html http://www.amazon.com/Hacking-Exposed-5th-Stuart-McClure/dp/B0018SYWW0/ref=sr_1_1?ie=UTF8&s=books&qid=1251593453&sr=1-1 http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html	People/Social Engineering/Audits	Cyber Security; Training & Awareness; Human Resources; Security Systems;	1	1	1	1	1	1	1	1	1	0	0	3
New	**Firewall Protection:** Service Providers & Network Operators should utilize firewall protection on all computing devices.: Whenever available for a mobile communications device, firewall software should be installed and utilized.	Source: http://www.k-state.edu/its/security/procedures/mobile.html	People/Data Loss-Leakage/Access Protection	Cyber Security; Security Systems;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Data Leakage:** Service Providers and Network Operators should develop employee education programs that emphasize the need to comply with policies and the DLP program.	Source: http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/06/15/laptop-encryption-software-for-social-security-administration-telecommuters.aspx	People/Data Loss-Leakage/Awareness	Cyber Security; Training & Awareness;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Data Leakage:** Service Providers and Network Operators should have and enforce disciplinary programs for employees who do not follow Data Loss Prevention (DLP) Guidelines.	Source:http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/06/15/laptop-encryption-software-for-social-security-administration-telecommuters.aspx	People/Data Loss-Leakage/Enforcement	Cyber Security; Training & Awareness;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Security Maturity and Metrics:** Network Operators, Service Providers and Equipment Suppliers should measure the effectiveness of their Security programs.	http://ezinearticles.com/?Employee-Security-Awareness&id=4084497	People / Security Awareness/Measuring Effectiveness	Cyber Security; Training & Awareness; Information Protection	1	1	1	1	1	1	1	1	1	0	0	3

New	**Security Policy:** Network Operators and Service Providers should develop a detailed security policy addressing social engineering issues and enforce it throughout the company.	Source:http://www.windowsecurity.com/articles/Social_Engineers.html	People/Social Engineering/Securing Devices	Cyber Security; Training & Awareness; Information Protection	1	1	1	1	1	1	1	1	0	0	0	3
New	**Security Policy:** Network Operators, Service Providers and Equipment Suppliers should establish and enforce policy to lock up paperwork and magnetic media containing confidential information and destroy it when it is no longer needed.	Source:http://www.windowsecurity.com/articles/Social_Engineers.html	People/Social Engineering/Securing Devices	Cyber Security; Training & Awareness; Information Protection	1	1	1	1	1	1	1	1	1	0	0	3
New	**Security Policy:** Network Operators, Service Providers and Equipment Suppliers should establish and enforce policy to physically secure the computers and network devices.	Source:http://www.windowsecurity.com/articles/Social_Engineers.html	People/Social Engineering/Securing Devices	Cyber Security; Training & Awareness; Information Protection; Policy; Physcial Security Management;	1	1	1	1	1	1	1	1	1	0	0	3
New	**Identity Administration:** Network Operators and Service Providers should have procedures for verifying identity of users to IT department and IT personnel to users (secret PINs, callback procedures, etc.).	Source:http://www.windowsecurity.com/articles/Social_Engineers.html	People/Social Engineering/Password Polices	Cyber Security; Training & Awareness; Information Protection; Policy; Access Control;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Identity Administration:** Network Operators and Service Providers should establish and enforce policy to prohibit disclosing passwords, to whom (if anyone) passwords can be disclosed and under what circumstances, procedure to follow if someone requests disclosure of passwords.	Source:http://www.windowsecurity.com/articles/Social_Engineers.html	People/Social Engineering/Password Polices	Cyber Security; Training & Awareness; Information Protection; Policy; Access Control;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Physical Security:** Network Operators and Service Providers should establish and enforce policy to require users to log off, to use password protected screensavers when away from the computer, enable screenlock upon activity timeout, cautionary instructions on ensuring that no one is watching when you type in logon information, etc. Physical security measures to prevent visitors and outside contractors from accessing systems to place key loggers, etc.	Source:http://www.windowsecurity.com/articles/Social_Engineers.html	People/Social Engineering/Password Polices	Cyber Security; Training & Awareness; Information Protection; Policy; Access Control;Physical Security Management;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Security Policy:** Network Operators and Service Providers should establish clear guidelines and policy on the corporate use of Social Media outlets. Before utilizing social media in any capacity, stop and consider the motivation of those that you are interacting with or targeting.	Source: Social Engineering Newsletter Volume 2, issue 7 http://www.social-engineer.org/Newsletter/SocialEngineerNewsletterVol02Is07.htm	People/Social Engineering/Social Media Outlets	Cyber Security; Training & Awareness; Information Protection; Policy;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Identity Administration:** Network Operators and Service Providers should establish policies governing destruction (shredding, incineration, etc.) of paperwork, disks and other media that hold information a hacker could use to breach security.	Source: 2009 Carnegie Mellon University, Author: Mindi McDowell posted on: http://www.us-cert.gov/cas/tips/ST04-014.html	People/Social Engineering/Safeguard the environment and network.	Cyber Security; Training & Awareness; Information Protection; Policy;	1	1	1	1	1	1	1	1	0	0	0	3

NRIC 7-7-8100 Changed	**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.	NIST Special Publication 800-53, Revision 3, Control Number AT-3 Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.	People/Awareness/ Training and Exercise	Cyber Security; Training & Awareness; Information Protection; Policy;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8124 Changed	**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	People/Awareness/Security Awareness	Cyber Security; Training & Awareness; Information Protection; Policy;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8125 Changed	**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.	ISO 27002 Information Security Standards - 8.1.3 Terms and conditions of employment	People/Security/Policy	Cyber Security; Training & Awareness; Policy;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8519 Changed	**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.		People/Security/Policy	Cyber Security; Training & Awareness; Policy; Human Resouces;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8092 Changed	**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).	People/Security/Policy	Cyber Security; Training & Awareness; Policy; Human Resouces;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-7-8099 Changed	**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.		People/Security/Policy	Cyber Security; Policy; Human Resouces;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-6-8096 Unchanged	**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.	People/Awareness/Security Awareness	Cyber Security; Policy; Security Systems; Training and Awareness;	1	1	1	1	1	1	1	1	0	0	0	3

New	**Third Party and Supply Chain Management:** Service Providers, Network Operators, and Equipment Suppliers should ensure supply chain security by having security language in their contracts and periodic risk assessments on their 3rd party verifing the outside party's security practices.	NIST 800-53 revision 3: Recommended Security Controls for Federal Information Systems and Organizations security control catalogue. NIST IR-7622, DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1	People/Supply Chain	Cyber Security; Policy; Training and Awareness;	1	1	1	1	1	1	1	1	1	0	0	3

New	**20**
Modified	**9**
Original	**7**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7-6-8071 changed	**Media Gateways Signaling:** Service Providers and Network Operators implementing a control-signaled (i.e. SIP) network should consider using media gateway controllers according to appropriate industry standards (i.e. Internet Engineering Task Force (IETF)) in order to achieve interoperability between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks.		Legacy Services / Media Gateways	Cyber Security; Network Design;Network Interoperability;	1	1	0	0	1	0	1	1	0	0	0	3
New	**Media Gateway Availability:** Network Operators and Service Providers should engineer networks to provide redundant and highly available application layer services. (e.g., DNS and other directory services, SIP, H.323).		Legacy Services / Media Gateways	Cyber Security; Network Design;Network Interoperability;	1	1	0	0	1	0	1	1	0	0	0	3
New	**Media Gateway Interoperability:** Network Operators and Service Providers should implement applicable industry standards governing protocol (e.g., IP Protocols from the IETF) and established policies and procedures to maintain currency within these publications to ensure interoperability.		Legacy Services / Media Gateways	Cyber Security; Network Design;Network Interoperability;	1	1	0	0	1	0	1	1	0	0	0	3
New	**Media Gateway Interoperability With Legacy Networks:** Network Operators and Service Providers implementing a signaling gateway should consider using media gateway controllers that map gateway responses to SS7 in an anticipated and predictable fashion (e.g., RFC 3398 for SIP-to-SS7 mapping).		Legacy Services / Media Gateways	Cyber Security; Network Design;Network Interoperability;	1	1	0	0	1	0	1	1	0	0	0	3
New	**Media Gateway Codecs:** Network Operators and Service Providers should use a minimum interworking subset for encoding standards (e.g., a fallback to G.711) in a PSTN gateway configuration in order to achieve interoperability and support all types of voice band communication (e.g., DTMF tones, facsimile, TTY/TDD).		Legacy Services / Media Gateways	Cyber Security; Network Design;Network Interoperability;	1	1	0	0	1	0	1	1	0	0	0	3
New	**CALEA Distribution:** Network Operators and Service Providers should establish policies and procedures to limit the distribution of CALEA information, requests, and network documents regarding CALEA interfaces to those operationally involved with CALEA activities.		Legacy Services / CALEA	Cyber Security; Network Design;Network Interoperability; Policy;	1	1	0	0	1	0	1	1	0	0	0	3
New	**CALEA Risk Assessment:** Network Operators and Service Providers should establish policies and procedures to periodically conduct risk assessments of CALEA procedures and policies.		Legacy Services / CALEA	Cyber Security; Policy;	1	1	0	0	1	0	1	1	0	0	0	3

New	**CALEA Access and Authorization:** Network Operators and Service Providers should establish policies and procedures to limit access to captured or intercepted CALEA content to those who are authorized.		Legacy Services / CALEA	Cyber Security; Policy;	1	1	0	0	1	0	1	1	0	0	0	3
New	**CALEA Awareness:** Network Operators and Service Providers should establish policies and procedures to promote awareness of appropriate CALEA policies among network employees and equipment vendors.		Legacy Services / CALEA	Cyber Security; Policy;	1	1	0	0	1	0	1	1	0	0	0	3
New	**GSM MAP Signaling and Network** Management: Wireless Service Providers and Network Operators who have deployed IS-41 (ANSI-41) or GSM Mobility Application Part (MAP) signaling networks should consider equipping their networks with network management and congestion controls.		Legacy Services / Signal Control Points	Cyber Security; Network Design;Network Interoperability;	1	1	1	0	1	0	1	1	0	0	0	3
New	**Signaling Policies:** Network Operators should implement rigorous screening and/or filtering on both internal and interconnecting signaling links and establish policies to review and improve screening capabilities.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Design;Network Interoperability;	1	1	0	0	1	0	0	1	0	0	0	3
New	**Signaling on General Purpose Computers:** Network Operators and Equipment Vendors of products built on general purpose computing products should proactively monitor all security issues associated with those products and cooperatively identify and apply security fixes, as necessary.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Hardware; Network Elements;	1	1	0	0	1	0	0	1	1	0	0	3
New	**Signaling Over Public IP:** Network Operators should be particularly vigilant with respect to signaling traffic delivered by or carried over Internet Protocol networks. Network Operators that utilize the Public Internet for signaling, transport, or maintenance communications should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Hardware; Network Elements; Security Sytems;	1	1	0	0	1	0	0	1	0	0	0	3
New	**Signaling Authentication:** Network Operators should consider enabling logging for element security related alarms on network elements, (e.g., unauthorized access, unauthorized logins, logging of changes (i.e. configuration and translation), administrative access logging), and establish review policies for these records to mitigate network element authentication vulnerabilities.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Elements; Security Sytems; Network Operations;	1	1	0	0	1	0	0	1	0	0	0	3
New	**Network Element Access:** Network Operators utilizing dial-up connections for maintenance access to Network Elements should consider implementing dial-back modems with screening lists, communication encryptions (i.e. VPN's) and token based access control.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Elements; Security Sytems; Network Operations;	1	1	0	0	1	0	0	1	0	0	0	3

New	**Signaling DoS Protection:** Network Operators should establish alarming thresholds for various message types to ensure that DoS conditions are recognized. Logs should be maintained and policies established to improve screening and alarming thresholds for differentiating legitimate traffic from DoS attacks.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Elements; Network Operations;	1	1	0	0	1	0	0	1	0	0	0	3
New	**Signaling Network Design:** Network Operators should design their signaling network elements and interfaces consistent with applicable industry security guidelines and policies (e.g. ATIS-300011).		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Elements; Network Operations; Policy	1	1	0	0	1	0	0	1	0	0	0	3
New	**Maintaining Physical Link Diversity:** Network Operators and Service Providers should implement industry guidelines for validating physical diversity, and consider performing signaling link diversification validation on a scheduled basis (e.g., twice a year). Processes and procedures should exist for tracking discrepancies and maintaining a historical record.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Elements; Network Operations; Hardware; Policy	1	1	0	0	1	0	1	1	0	0	0	3
New	**Maintaining Logical Link Diversity:** Network Operators who deploy next generation signaling networks should consider industry guidelines for logical diversity (e.g. multi-homing), and perform network diversification validation on a scheduled basis (e.g., twice a year). Processes and procedures should exist for tracking discrepancies and maintaining a historical record.		Legacy Services / Gateway to Gateway Protocol, Interoperability & Security Issues	Cyber Security; Network Elements; Network Operations; Network Interoperability;	1	1	0	0	1	0	0	1	0	0	0	3
New	**Signaling Services Requested Changes:** Network Operators should establish policies and processes for adding and configuring network elements, that include approval for additions and changes to configuration tables (e.g., screening tables, call tables, trusted hosts, and calling card tables). Verification rules should minimize the possibility of receiving inappropriate messages.		Legacy Services / Social Engineering	Cyber Security; Network Elements; Network Operations; Policy	1	1	0	0	1	0	0	1	0	0	0	1
New	**Logging of Requested Changes:** Network Operators should log changes made to network elements and consider recording the user login, time of day, IP address, associated authentication token, and other pertinent information associated with each change. Policies should be established to audit logs on a periodic bases and update procedures as needed.		Legacy Services / Social Engineering	Cyber Security; Network Elements; Network Operations; Policy	1	1	0	0	1	0	0	1	0	0	0	2
New	**Non-Repudiation:** Network Operators should establish policies and procedures to ensure that actions taken on the network can be positively attributed to the person or entity that initiated the action. This may include, but is not limited to electronic logging, access control, physical records, or tickets.		Legacy Services / Social Engineering	Cyber Security; Network Elements; Network Operations; Policy	1	1	0	0	1	0	0	1	0	0	0	3

NRIC 7-6-8051 Changed	**Network Access Control for SS7:** Network Operators should ensure that SS7 signaling interface points that connect to the IP Private and Corporate networks interfaces are well hardened, protected with packet filtering firewalls; and enforce strong authentication. Similar safeguards should be implemented for e-commerce applications to the SS7 network. Network Operators should implement rigorous screening on both internal and interconnecting signaling links and should investigate new, and more thorough screening capabilities. Operators of products built on general purpose computing products should proactively monitor all security issues associated with those products and promptly apply security fixes, as necessary. Operators should be particularly vigilant with respect to signaling traffic delivered or carried over Internet Protocol networks. Network Operators that do employ the Public Internet for signaling, transport, or maintenance communications and any maintenance access to Network Elements should employ authentication, authorization, accountability, integrity, and confidentiality mechanisms (e.g., digital signature and encrypted VPN tunneling).	ITU SS7 Standards, "Securing SS7 Telecommunications Networks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 5-6 June 2001.	Legacy Services / SS7	Cyber Security; Network Elements; Network Operations; Policy	0	1	0	0	0	0	0	1	0	0	0	1
NRIC 7-6-8052 Changed	**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	NIIF Guidelines for SS7 Security.	Legacy Services / SS7	Cyber Security; Network Elements; Network Operations;	0	1	0	0	0	0	0	1	0	0	0	2

NRIC 7-6-8054 Changed	**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.		Legacy Services / SS7	Cyber Security; Network Elements; Network Operations; Policy	0	1	0	0	0	0	0	1	0	0	0	2
NRIC 7-7-8534 Changed	**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.		Legacy Services / SS7	Cyber Security; Network Elements; Network Operations;	0	1	0	0	0	0	1	1	0	0	0	3
NRIC 7-6-8053 Changed	**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.		Legacy Services / SS7	Cyber Security; Network Elements; Network Operations;	0	1	0	0	0	0	0	1	0	0	0	3

NRIC 7-7-0551 Changed	**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	Legacy Services / SS7	Cyber Security; Network Elements; Network Operations; Network Interoperability;	0	1	0	0	0	0	0	1	0	0	0	3

New	**21**
Modified	**7**
Original	**0**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Sub domain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
New	**General:** Service Providers should classify identity management services against the service architecture and deployment model being utilized to determine the general "security" posture of the identity services, how it relates to asset's assurance and security protection requirements, and define the needed security architecture to mitigate security risks. Specifically, if identity related functions are distributed among multiple parties, all parties involved should be clearly identified (e.g., relying parties such as users and service providers, credential providers, verifier or authentication providers, or federation members) with clearly defined roles, responsibilities, and accountability for the security of the identity service and all associated assets.	ITU-T X.1250, *Baseline capabilities for enhanced global identity management and interoperability* NIST SP 800-63, *Electronic Authentication Guideline*	Identity Mgmt / Lifecycle	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	3
New	**Federated Identity:** If identity is being federated (i.e., for use among members of a federation), Service Providers should clearly define and enforce rules, policies and trust model for the federated identity services.		Identity Mgmt / Lifecycle	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	3
New	**Identity Data Security –** Service providers creating, maintaining, using or disseminating individually identifiable information should take appropriate measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse or alteration. Organizations should take reasonable steps to assure that third parties to which they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect any transferred information.	Liberty Alliance Project, Privacy and Security Best Practices Version 2.0	Identity Mgmt / Lifecycle	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	3

New	**Identity Data Quality and Access:** Service Providers creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used. Organizations should establish appropriate processes or mechanisms so that inaccuracies in material individually identifiable information, such as account or contact information, may be corrected. These processes and mechanisms should be simple and easy to use, and provide assurance that inaccuracies have been corrected. Other procedures to assure data quality may include use of reliable sources and collection methods, reasonable and appropriate access and correction, and protections against accidental or unauthorized alteration.	Liberty Alliance Project, Privacy and Security Best Practices Version 2.0	Identity Mgmt / Lifecycle	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC 7-6-8071	**Identity Lifecycle Management:** Service Providers should clearly define and enforce policies for identity lifecycle management. This includes processes, procedures and policies for the proofing, enrolling, issuing and revoking of identity information (e.g., identifiers, credentials and attributes) to be used for a specific context (e.g., for specific transactions ranging from commercial to social activities).	ITU-T Y.2720, *NGN Identity Management Framework* ITU-T Y.2721, *NGN Identity Management Requirements and Use Cases* ATIS-1000035, *NGN Identity Management Framework*	Identity Mgmt / Access Control	Cyber Security; Identity Mgmt; Access Control; Policy;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC7-7-8502	**Identity Enrollment and Issuance:** Service Providers should only issue the identity information (e.g., identifiers, credentials and attributes) associated with an identity after successful identity proofing of the entity. An entity requesting enrolment should be verified and validated according to the requirements of the context (i.e., in which the identity will be used) before enrolling or issuing any associated identifiers, credentials or attributes. The proofing process and policies should be based on the value of the resources (e.g., services, transactions, information and privileges) allowed by the identity and the risks associated with an unauthorized entity obtaining and using the identity. Specifically, measures to ensure the following is recommended: (a) An entity (e.g., person, organization or legal entity) with the claimed attributes exists, and those attributes are suitable to distinguish the entity sufficiently according to the needs of the context. (b) An applicant whose identity is recorded is in fact the entity to which the identity is bound; (c) It is difficult for an entity which has used the recorded identity and credentials to later repudiate the registration/enrolment and dispute an authentication.	ITU-T Y.2720, *NGN Identity Management Framework* ITU-T Y.2721, *NGN Identity Management Requirements and Use Cases* ATIS-1000035, *NGN Identity Management Framework*	Identity Mgmt / Access Control	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	1

NRIC7-7-8109	**Identity Maintenance and Updates:** Service Providers should ensure secure management and maintenance of the identity data and the status of data (e.g., identifiers, credentials, attributes) by logging updates or changes to an identity, provide notifications about the updates or changes to an identity(s) or any of the data associated with the identity(s) to the systems and network elements that needs to be aware of the updates or changes, and by periodically validating the status of an identity.	ITU-T Y.2720, *NGN Identity Management Framework* ITU-T Y.2721, *NGN Identity Management Requirements and Use Cases* ATIS-1000035, *NGN Identity Management Framework*	Identity Mgmt	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	1
NRIC 7-6-8023	**Identity Revocation:** Service Providers should have applicable polices and enforcement for revoking an identity. Specifically, (a) Enforce policies and terminate or destroy the credentials associated (e.g., digital certificates or tokens) with an identity when it is no longer valid or has a security breach. (b) Provide notifications about the revocation or termination of an identity(s) or any of the data associated with the identity to the entity and to the systems and network elements that needs to be aware (i.e., All systems and processes with which the identity can be used for access have to be notified that the identity is no longer valid).	ITU-T Y.2720, *NGN Identity Management Framework* ITU-T Y.2721, *NGN Identity Management Requirements and Use Cases* ATIS-1000035, *NGN Identity Management Framework*	Identity Mgmt / Access Control	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	1
New	**Identity Information Access Control:** Service Providers should ensure that identity information is only be accessible to authorized entities subject to applicable regulation and policy. Specifically, (a) an entity (e.g., relying party or requesting party) requesting identity data should be authenticated, and its authorization to obtain the requested information verified before access to the information is provided or the requesting identity data is exchanged. (b) policy and rules for requesting and exchanging identity data among multiple parties involved (e.g., users, relying party and identity provider) should be clearly defined and enforced.	ITU-T Y.2720, *NGN Identity Management Framework* ITU-T Y.2721, *NGN Identity Management Requirements and Use Cases* ATIS-1000035, *NGN Identity Management Framework*	Identity Mgmt	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	1

NRIC 7-7-8019	**Multi-factor Authentication:** Service Providers and Network Operators should support multi-factor authentication to increase confidence in the identity of an entity. Multi-factor authentication involves validating the authenticity of the identity of a entity by verifying multiple identifiers and attributes associated with the entity. The data for multi-factor authentication capabilities should be organized based something you are (e.g., physical of behavioral characteristics of a end user or customer's characteristic or attribute that is being compared such as typing patterns, voice recognition), something you have (e.g., a driver's license, or a security token) and something you know (e.g., a password, pin number, security image).	ITU-T Y.2702, *Authentication and authorization requirements for NGN release 1* ATIS-1000030, *Authentication and Authorization Requirements for Next Generation Network (NGN)* NIST SP 800-63, *Electronic Authentication Guideline*	Identity Mgmt / Strong Authentication	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	2
NRIC 7-7-8084 Unchanged	**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.	Identity Mgmt / Certificates	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8020	**Protection of Personally Identifiable Information (PII):** Service Providers should protect Personally Identifiable Information by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. Policies for PII protection should be clearly identified and enforced. Specifically, (a) Organizations should identify all PII residing in their environment. (b) Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to reduce the likelihood of harm caused by a breach involving PII. Also, an organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission. For example, organizations could have an annual PII purging awareness day. (c) Organizations should categorize their PII based on confidentiality impact levels. For example, PII confidentiality impact level—low, moderate, or high should be used to indicate the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. (d) Organizations should apply the appropriate safeguards for PII based on the PII	NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*	Identity Mgmt	Cyber Security; Identity Mgmt; Access Control; PII	1	1	1	1	1	1	1	0	0	0	0	2

New	**SAML Privacy:** Service Providers should analyze each of the steps in the interaction (and any subsequent uses of data obtained from the transactions) of a Security Assertion Markup Language (SAML) transaction to ensure that information that should be kept confidential is actually being kept so.	OASIS, *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*	Identity Mgmt	Cyber Security; Identity Mgmt; Access Control; Privacy;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC 7-6-8032	**SAML Communications:** Service Providers should use secure network protocols such as TLS or IPsec should be used to provide integrity and confidentiality protection of SAML communications. In addition, the following measures should be implemented to counter replay, denial of service and other forms of attacks: (a) Clients should be required to authenticate at some level below the SAML protocol level (for example, using the SOAP over HTTP binding, with HTTP over TLS/SSL, and with a requirement for client-side certificates that have a trusted Certificate Authority at their root) to provide traceability and counter DOS attacks. (b) Use of the XML Signature element <ds:SignatureProperties> containing a timestamp should be required to determine if a signature is recent to counter replay attacks. (c) Maintaining state information concerning active sessions, and validate correspondence. (d) Correlation of request and response messages.	OASIS, Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0	Identity Mgmt / SAML	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC 7-8-8081 Unchanged	**Enforcable Password Policy:** Network Operators, Service Providers and Equipment Suppliers should develop an enforceable password policy, which considers different types of users, requiring users to protect, as applicable, either (a) the passwords they are given/create or (b) their credentials for two-factor authentication.		Identity Mgmt / Strong Authentication Methods	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8085 Changed	**Expiration of Digital Certificates:** 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, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 341-389.	Identity Mgmt / Certificates	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8120 Changed	**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.		Identity Mgmt / Certificates	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-7-8138 Changed	**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.		Identity Mgmt / Certificates	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	2
NRIC 7-7-8500 Changed	**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.	NIST SP800-57 Recommendation for key management http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf	Identity Mgmt / Certificates	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8501 Changed	**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.	NIST SP800-57 Recommendation for key management http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf	Identity Mgmt / Certificates	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8079 Changed	**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	Identity Mgmt / Password	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	2

NRIC 7-7-8080 Changed	**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/ - 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	Identity Mgmt / Password	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	2
NRIC 7-7-8081 Changed	**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/ - 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	Identity Mgmt / Password	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	2
New	**Password Management Policy:** Service Providers and Network Operators should define, implement, and maintain password management policies as well as the documented process to reduce the risk of compromise of password-based systems.	NIST SP800-118 Guide to Enterprise Password Management http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf	Identity Mgmt / Password	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	0	0	0	2
New	**Recovery from Password Management System Compromise:** When a password management system or other source of passwords has been compromised, the Service Provider should act swiftly to mitigate the weaknesses that allowed the compromise, restore the compromised system to a secure state, and require all users to change their passwords immediately. Procedures should be in place to notify all affected users that their passwords have been reset or need to be changed immediately.	NIST SP800-118 Guide to Enterprise Password Management http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf	Identity Mgmt / Password	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	0	0	0	0	2

NRIC 7-6-8014 Changed	**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/ - 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	Identity Mgmt / Role based access control	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	0	0	0	2
NRIC 7-7-8126 Changed	**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/ - 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	Identity Mgmt / Strong authentication	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	2
NRIC 7-6-8013 Changed	**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.	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 Requirements for the Management Plane: March 2008	Identity Mgmt / Systems administration	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8113 Changed	**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 Requirements for the Management Plane: March 2008	Identity Mgmt / Systems administration	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	1	1	1	1	0	0	3

New	**8**
Modified	**12**
Original	**9**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7-7-8001 Changed	**Strong Encryption Algorithms and Keys:** Service Providers, Network Operators, and Equipment Suppliers should use industry-accepted published guidelines specifying algorithms and key lengths for all uses of encryption, such as 3DES or AES.	Reference: http://www.atis.org/ - T1 276-2008 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	Encryption / Encryption Keys	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	1	1	0	3
NRIC 7-6-8028 Unchanged	**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, and b) Cannot be emulated by a non-trusted source, and c) includes processes for key revocation.		Encryption / Encryption Keys	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-6-8059 Unchanged	**Protect Cellular Data Channel:** Service Providers and Network Operators should encourage the use of encryption services of the cellular 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, LTE, etc.	Encryption / Cellular Network Encryption	Cyber Security; Encryption; Information Protection;	0	0	1	0	0	0	1	1	0	0	0	3
NRIC 7-6-8094 Unchanged	**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.	Encryption / Device Encryption	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC 7-7-8105 Changed	**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	Encryption / Voice Encryption	Cyber Security; Encryption; Information Protection;	0	0	1	0	0	0	1	1	0	0	0	1
New	**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	Encryption / Data Encryption	Cyber Security; Encryption; Information Protection;	1	1	0	0	1	0	1	1	0	0	0	1

NRIC 7-7-8503 Changed	**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 vulnerabilities are mitigated with proper and current 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	Encryption / Key Recovery	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	1	0	0	0	1
New	**Protection of Devices Beyond Scope of Control:** Equipment Suppliers should implement techniques such as tamper-proof crypto-chips/authentication credentials and (remote) authentication for (service provider) configuration controls, in customer premises equipment. Additionally, capabilities to remotely access or delete sensetive information on these devices is encouraged.	PacketCableTM Security Specification PKT-SP-SEC-I11-040730, IETF RFC 3261, Related to BP 8134	Encryption / Crypto-Authentication	Cyber Security; Encryption; Information Protection; Access Control;	1	1	1	1	1	1	0	0	1	0	0	3
New	**General:** Service Providers should use encryption to separate data in rest from data in motion.	Cloud Security Alliance (CSA)	Encryption / Cloud	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	3
New	**Key Management:** Service providers should segregate key management from the cloud provider hosting the data, creating a chain of separation. This protects both the cloud provider and customer from conflicts when compelled to provide data due to a legal mandate.	Cloud Security Alliance (CSA)	Encryption / Cloud	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	3
New	**Management:** Service providers should provide documentation and enforce role management and separation of duties.	Cloud Security Alliance (CSA)	Encryption / Cloud	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	3
New	**Key Management:** In cases where the cloud provider must perform key management, service providers should define processes for key management lifecycle: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Further, understand whether the same key is used for every customer or if each customer has its own key set.	Cloud Security Alliance (CSA)	Encryption / Cloud	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	1
New	**Public Key Infrastructure (PKI):** For environments where traditional PKI infrastructures are problematic, service providers should use an alternate approach such as a "web of trust" for public key validation / authenticaton.	Reference: http://en.wikipedia.org/wiki/Public_key_infrastructure Reference: SP800-45 (NIST) http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf Guidelines on Electronic Mail Security	Encryption / Identity Mgmt	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	3

New	**Layered Encryption:** Where possible, service providers should use layered VPN and encryption strategies to mitigate device vulnerabilities. Traditionally a single layer of cryptography has stood between the data being protected and that of the attacker. While the cryptography itself is rarely the weak link, many times implementation or other originating or terminating cryptographic device vulnerabilities places that information in jeopardy.		Encryption / Layered Approach	Cyber Security; Encryption; Information Protection; Network Operations;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC 7-7-8001 Changed	**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/ - 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	Encryption / Standards	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-6-8059 Unchanged	**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.	Encryption / Wireless Networks	Cyber Security; Encryption; Information Protection;	0	0	1	0	0	0	1	1	0	0	0	2
NRIC 7-6-8094 Changed	**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.	Encryption / Device Encryption	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	0	0	0	0	3
NRIC 7-7-8111 Changed	**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.		Encryption / Data Encryption	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-7-8026 Changed	**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	Encryption / Key Management	Cyber Security; Encryption; Information Protection;	1	1	1	1	1	1	1	1	1	0	0	1

New	**8**
Modified	**7**
Original	**4**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7-6-8071 Changed "Service Providers and Network Operators" to "System Owners and the Security Team"	**Threat Awareness:** Service providers and Network Operators should subscribe to vendor patch/security notifications and services to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network.	NIST SP 800-40 v2.0 Creating a Patch and Vulnerability Management Program Dependency on NRIC BP 8034 and 8035.	Vulnerability Mgmt / Alerting	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8137 Unchanged	**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.	Vulnerability Mgmt / Alerting	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	0	0	1	0	0	3
NRIC 7-7-8119 Changed	**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.		Vulnerability Mgmt / Alerting	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8502 Changed	**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	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	1
7-6-8023 Unchanged	**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.	NIST SP 800-115 A Technical Guide to Information Security Testing and Assessement, NIST SP 800-40 v2.0 Creating a Patch and Vulnerability Management Program	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	1
New	**Security Testing on New Devices and Infrastructure:** Service providers, network operators, and equipment vendors should test new devices to identify unneccesary services, outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy prior to being placed on a network.	NIST SP 800-115 A Technical Guide to Information Security Testing and Assessement	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	1	0	0	1

New	**Risk Assessment Process:** Service providers and network operators should have documented processes in place for reviewing new vulnerabilities as they are announced.	Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 8 -10.	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	3
New	**Risk Assessments:** Service providers and network operators should have assigned risk ratings for vulnerabilities and definitions of those risk ratings (i.e. What does a High risk vulnerability mean to the general user public?, etc.) Finally the security team should have access to an accurate and readily available asset inventory (See Step 1: Asset Inventory) (including the asset owners, and patch levels) and network diagrams.	Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 8 - 10.	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	3
New	**Vulnerability Assessment Scans:** Service Providers and Network Operators should test new tools in a lab to identify any false positives and false negatives and use a change control system in case there is a network disruption. They should use a tool that causes minimal disruptions to the network	Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 11, 12.	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt	1	1	1	1	1	1	1	1	0	0	0	2
New	**Vulnerability Assessment Policies:** Service providers, network operators, and equipment vendors should use custom policies created by OS, device, or by industry standard (SANS Top 20, Windows Top 10 Vulnerabilities, OWASP Top 10) and specific to your environment. Organizations should identify what scanning methods and operating procedures are best for their company, and document how they would proceed in a standard operating procedure.	Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 11, 12.	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt; Policy	1	1	1	1	1	1	1	1	1	0	0	1
New	**Reporting and Remediation Tracking Tools:** Service Providers and Network Operators should ensure the tools they use are capable of notifying the asset owners that they have vulnerabilities to be fixed. They should be able to provide high-level dashboard type reports to senior management and detailed host reports to system administrators.	Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 12 - 13.	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt;	1	1	1	1	1	1	1	1	0	0	0	3
New	**Vulnerability Reporting and Remediation:** Service providers, network operators, and equipment vendors should focus on the highest risk vulnerabilities by ranking them by the vulnerability risk rating.	Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 12, 14.	Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt;	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-7-8139 Changed	**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.		Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt;	1	1	1	1	1	1	1	1	0	0	0	2
NRIC 7-6-8023 Unchanged	**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.		Vulnerability Mgmt / Risk & Vulnerability Assesment	Cyber Security; Vulnerabiity Mgmt;	1	1	1	1	1	1	1	1	0	0	0	1
7-7-8000 Unchanged	**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	Vulnerability Mgmt / Mitigation	Cyber Security; Vulnerabiity Mgmt;	1	1	1	1	1	1	1	1	1	0	0	1
7-7-8004 Unchanged	**Harden Default Configurations:** Equipment Suppliers should work closely and regularly with US-CERT/NCCIC, 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	Vulnerability Mgmt / Mitigation	Cyber Security; Vulnerabiity Mgmt; Network Operations	1	1	1	1	1	1	0	0	1	0	0	2
7-7-8019 Unchanged	**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. Hardening procedures include (a) all unnecessary services are disabled; (b) all unnecessary communications pathways are disabled; (c) all critical security patches have been evaluated for installations on said systems/applications; and d) review and implement published hardening guidelines, as appropriate. Where critical security patches cannot be applied, compensating controls should be implemented.	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	Vulnerability Mgmt / Mitigation	Cyber Security; Vulnerabiity Mgmt; Network Operations	1	1	1	1	1	1	1	1	1	0	0	1

7-7-8056 Unchanged	**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.	Vulnerability Mgmt / Mitigation	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	0	0	1	0	0	0	3
7-6-8057 Unchanged	**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.	Vulnerability Mgmt / Mitigation	Cyber Security; Identity Mgmt; Access Control;	1	1	1	1	1	0	0	0	1	0	0	3
7-7-8106 Changed to be more comprehensive.	**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	Vulnerability Mgmt / Mitigation	Cyber Security; Vulnerabiity Mgmt; Network Operations	1	1	1	1	1	1	1	1	1	0	0	1
7-7-8505 Unchanged	**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	Vulnerability Mgmt / Mitigation	Cyber Security; Vulnerabiity Mgmt; Network Operations	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8103 Changed	**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.	NIST SP800-83 Guide to malware incident prevention and handling http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf 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.	Vulnerability Mgmt / Mitigation	Cyber Security; Vulnerabiity Mgmt; Network Operations; Security Systems;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8020 Changed	**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.	Configuration guide for security from NIST (800-53 Rev. 3).	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-6-8032 Changed	**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.	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	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt	1	1	1	1	1	1	1	1	1	0	0	3
NRIC 7-7-8034 Changed	**Software Patching Policy:** Service Providers and Network Operators should define and incorporate a formal patch/fix policy into the organization's security policies.	Configuration guide for security from NIST (800-53 Rev. 3).	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt; Policy;	1	1	1	1	1	1	1	1	0	0	0	2
NRIC 7-6-8035 Changed	**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.	Configuration guide for security from NIST (800-53 Rev. 3). Related to NRIC BP 8020.	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt; Policy;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-6-8036 Changed	**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.	Configuration guide for security from NIST (800-53 Rev. 3).	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt; Policy;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-6-8039 Changed	**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.	Configuration guide for security from NIST (800-53 Rev. 3).	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8505 Changed	**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.	Configuration guide for security from NIST (800-53 Rev. 3).	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt;	1	1	1	1	1	1	1	1	1	0	0	2
NRIC 7-7-8566 Changed	**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.	Configuration guide for security from NIST (800-53 Rev. 3).	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt;	1	1	1	1	1	1	1	1	0	0	0	2

New	**Version Control Systems:** Service providers, network operators, and equipment suppliers should automated (where possible) Patch Management to quickly deploy patches for known vulnerabilites	NIST Special Publication 800-40, Creating a Patch and Vulnerability Management Program - 2.1 Recommended Process	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt;	1	1	1	1	1	1	1	1	1	0	0	3
7-6-8032 Changed to reference software patching policy.	**Patching Practices:** Service Providers, Network Operators, and Equipment Suppliers should design and deploy a well-defined patching process especially for critical OAM&P systems. These processes should be based on the Software Patching Policy.	NIST SP 800-40 v2.0 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	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt;	1	1	1	1	1	1	1	1	1	0	0	1
New	**General Patching:** Service providers and network operators should establish and implement procedures to ensure that all security patches and updates relevant to the device or installed applications are promptly applied. The patching process should be automated whenever possible. The system should be rebooted immediately after patching if required for the patch to take effect.	Source: http://www.k-state.edu/its/security/procedures/mobile.html#summary	Vulnerabiity Mgmt / Patch Management	Cyber Security; Vulnerabiity Mgmt; Network Operations; Patch Mgmt;	1	1	1	1	1	1	1	1	0	0	0	1

New	**9**
Modified	**15**
Original	**9**

NRIC VII Cross Reference (New/Changed/Unchanged/Deleted)	CSRIC Best Practice	CSRIC Reference/Comments	Domain/Subdomain	Keywords	Cable	Wireline	Wireless	Satellite	Internet / Data	Broadcast	Service Provider	Network Operator	Equipment Supplier	Property Manager	Government	Priority
NRIC 7-7-8062 Unchanged	**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.	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8068 Changed	**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.	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-6-8-31 Changed	**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/ - 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	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness;	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-7-8085 Changed	**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.		Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8130 Changed	**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.	ISO 27002 Information Security Standards - 13.1.1 Reporting information security events	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Training & Awareness;	1	1	1	1	1	1	1	1	1	0	0	2
New	**Incident Response Preventative Measures:** Service providers and network operations should set policy within each corporation or agency to provide guidance when there is a security breach.	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Training & Awareness; Policy	1	1	1	1	1	1	1	1	1	0	0	3
New	**Post DoS Practice:** Network Operators and Service Providers should establish policies, and procedures to support early recognition and isolation of potential bad actors to minimize impact to the network.	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Training & Awareness; Policy; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-6-8061 Changed	**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.	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Training & Awareness; Business Continuity; ; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8067 Unchanged	**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	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Training & Awareness; Business Continuity; ; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1

NRIC 7-7-8554 Changed	**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	Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8556 Changed	**Recovery from the Absence of a Monitoring Requests Policy:** In the absence of a monitoring request policy, Service Providers and Network Operators should refer all communications intercept requests to corporate counsel.		Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	2
NRIC 7-7-8557 Changed	**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.		Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8070 Changed	**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."		Incident Response / Policy & Plan	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	3
NRIC 7-7-8074 Changed	**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.		Incident Response / Prevention	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-7-8075 Changed	**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.		Incident Response / Prevention	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	2
NRIC 7-7-8076 Unchanged	**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.	Incident Response / Prevention	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	0	0	1	0	0	2
NRIC 7-7-8118 Changed	**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)	Incident Response / Prevention	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8559 Changed	**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).	NIST SP800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf	Incident Response / Prevention	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8110 Unchanged	**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	Incident Response / Attack Detection,	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-0507 Unchanged	**Analysis and Detection:** Network Operators, Service Providers and Equipment Supplies 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 traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purposes of consumer resources of a destination of network to block service or consume resource to overflow state that might cause system crashes).	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Attack Detection,	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-7-8567 Unchanged	**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.		Incident Response / Attack Detection	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8064 Changed	**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).		Incident Response / Attack Detection	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8510 Unchanged	**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	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8514 Changed	**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.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8515 Changed	**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.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8523 Changed	**Recovery from Network Element Resource Saturation Attack:** If the control plane is under attack, Service Providers and Network Operators should: 1) Turn on logging where appropriate to 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.	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1

NRIC 7-7-8527 Changed	**Recover from Compromised DNS (Domain Name System) Servers or Name Record Corruption:** If the DNS (Domain Name System) server has been compromised or the name records corrupted, Service Providers and Network Operators should first flush the DNS cache and, failing that, 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"	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
New	**Recover from Unauthorized Use:** Network Operators and Service Providers should remove invalid records whenever it is determined that a network element has been modified without proper authorization, or rollback to the last valid version of record. The attack should be investigated to identify potential security changes.	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	2
New	**Recover from Voice over IP (VoIP) Compromise:** If a Voice over IP (VoIP) server has been compromised, Service Provider and Network Operators should remove the device from the network until remediated.	PacketCable Security specification.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
New	**Recover from Voice over IP (VoIP) Device Masquerades or Voice over IP (VoIP) Server Compromise:** If a VoIP masquerading event is occuring the service provider or network operator should attempt to collect data via log files or other means to aid law enforcement investigations If VoIP device masquerading is causing significant harm, the portion of the network where the attack is originating can be isolated.	PacketCable Security specification.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8537 Changed	**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.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1

NRIC 7-7-8564 Changed	**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.	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
New	**Recover from DoS Attack:** Network Operators and Service Providers should work together to identify, filter, and isolate the originating points of Denial of Service (DoS) attacks when detected, and reroute legitimate traffic in order to restore normal service.	IETF RFC2350, CMU/SEI-98-HB-001.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8532 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8540 Changed	**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.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8528 Changed	**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"	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1

NRIC 7-7-8530 Changed	**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.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8533 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	0	1	0	0	0	0	1	1	0	0	0	1
NRIC 7-7-8539 Changed	**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.	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	0	0	1	0	0	0	1	1	0	0	0	1
NRIC 7-7-8561 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1

NRIC 7-7-8562 Changed	**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).		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8563 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	0	0	1	0	0	1
NRIC 7-7-8517 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8549 Changed	**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	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations; Disaster Recovery;	1	1	1	1	1	1	1	1	0	0	0	1
NRIC 7-7-8551 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1

NRIC 7-7-8553 Changed	**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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8555 Changed	**Recovery from Lack of an Incident Communications Plan:** If an 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.		Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	1	0	0	1
NRIC 7-7-8513 Changed	**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)	Incident Response / Response & Mitigation	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations;	1	1	1	1	1	1	1	1	0	0	0	1

New	**Recovery from Password Management System Compromise:** When a password management system or other source of passwords has been compromised, the Network Operator should act swiftly to mitigate the weaknesses that allowed the compromise, restore the compromised system to a secure state, and require all users to change their passwords immediately. Procedures should be in place to notify all affected users that their passwords have been reset or need to be changed immediately.	NIST SP800-118 Guide to Enterprise Password Management http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf	Identity Mgmt / Password	Cyber Security; Incident Response; Emergency Preparedness; Business Continuity; Network Operations; Access Control;	1	1	1	1	1	1	0	1	0	0	0	1

New	**7**
Modified	**35**
Original	**7**