March 2013

Working Group 11

Consensus
Cyber Security
Controls

Final Report

Final Report

Consensus Cyber Security Controls

March 6, 2013

WORKING GROUP 11 –
Consensus Cyber Security Controls

Table of Contents

1 Executive Summary

In August 2012, the Federal Communications Commission (FCC) indicated that it had recently become aware of the Twenty Critical Security Controls[1] (20 Controls) and convened Working Group 11 of the Communications, Security, Reliability, and Interoperability Council (CSRIC) to determine the applicability of the 20 Controls to the communications sector. To effectively manage the effort, the FCC emphasized that the focus of this activity is on protection of carrier and Internet Service Provider (ISP) network operations both directly and through enterprise systems connected to operational technology, but did not encompass customer premises equipment. Working Group 11 was tasked with comparing the 20 Controls with the CSRIC II best practices and determining which of the CSRIC II best practices might need to be added to the 20 Controls to enable them to deal with the attacks frequently launched against communications companies and their infrastructure.

Working Group 11 updated and reorganized the Cyber Security Best Practices that were last published in March 2011 as part of CSRIC II's Working Group 2A. The Working Group 2A effort leveraged a large body of cyber security best practices that were previously created by the Network Reliability and Interoperability Council (NRIC). Recognizing that many years had passed and that the "state-of-the-art" in cyber security has advanced rapidly since then, Working Group 2A took a fresh look at the cyber security best practices, including all segments of the communications industry and public safety communities. The Working Group 2A report noted that "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."

Working Group 11 continued the work related to one of Working Group 2A's key findings, specifically which, "in light of the current urgency" service providers and network operators "are encouraged to prioritize their review of these Best Practices and prioritize their timely, appropriate actions." Much has been accomplished in a relatively brief period of time by the participants in Working Group 11. By leveraging the work completed by numerous international and domestic agencies that produced the 20 Controls and by reviewing them in the context of carrier network operations, Working Group 11 successfully developed a similar set of critical controls that are relevant to the communications industry. By doing so, Working Group 11 was able to map the CSRIC II best practices under a revised control classification which resulted in a prioritized set of new best practices.

Working Group 11 recommends that the best practices list compiled by CSRIC II be modified to reflect the prioritized set of critical cyber security controls that have been identified to be applicable to the communications industry. Working Group 11 also recommends that the FCC support the industry's efforts to continue to develop, prioritize, and refine best practices that are consistent with evolving cyber-attacks and

[1] http://www.sans.org/critical-security-controls/

exploits, while ensuring that all participants in the ecosystem are equally vested in an appropriate approach to cyber security. Finally, Working Group 11 encourages the FCC to support current efforts within the United States (U.S.) government to avoid duplicative agency activities.

When Working Group 11 was convened, it was already late in the CSRIC III process, and some participants expressed concern that there may not be enough time to fully realize the goals of the Working Group. Accordingly, some participants received assurances that the core focus of Working Group 11 was to map the 397 best practices previously developed by Working Group 2A in CSRIC II to the subsequently developed list of 20 Controls for enterprises. Working Group 11 participants were committed and worked accordingly to ensure that at a minimum, a gap analysis could be completed during CSRIC III so as to be better prepared for future development and activity in this area. Accordingly, aspects of this report that go beyond the basic mapping and gap analysis, while laudable and useful in many respects, may not fully reflect consideration by all of the Working Group 11 members. It is recommended that future development of cyber security practices for the communications sector include efforts to have the conclusions and recommendations of the Working Group in the specific areas enumerated in Recommendation (c) be vetted, continually reviewed, and updated by a broad cross-section of communications sector industry participants.

2 Background

In February 2009 the Center for Strategic and International Studies (CSIS) published the first version of a consensus list of critical security controls – essential best practices that are known to block or mitigate the effect of cyber intrusions. Compiled jointly by representatives of the National Security Agency (NSA), Department of Homeland Security (DHS), the nuclear energy labs of the Department of Energy, the Department of Defense (DoD) Cyber Crime Center (DC3), the Joint Task Force-Global Network Operations (JTF-GNO) and many commercial organizations, these guidelines were unique because they were informed directly by in depth knowledge of all known attack vectors.

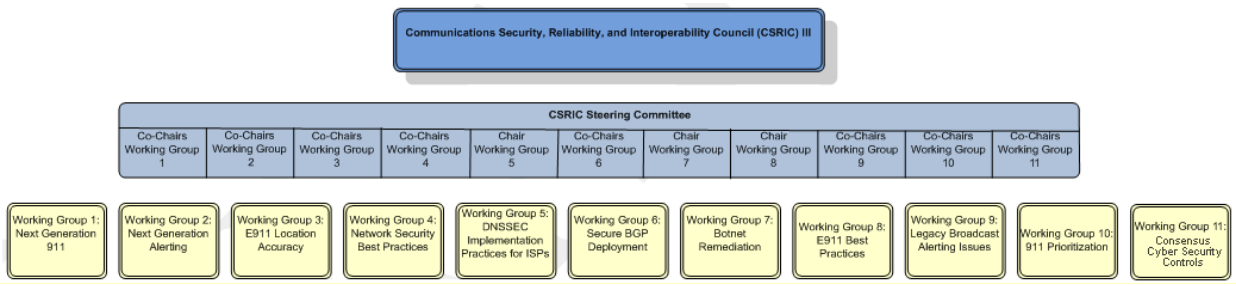
Three years and three updates later, the British and U.S. governments came together to jointly document the importance of these essential controls. As a result of this collaborative effort, the British Centre for the Protection of National Infrastructure (CPNI), the U.S. State Department and the U.S. DHS adopted the consensus best practices as the foundations for broad based initiatives to better protect the computers and networks that serve their respective national governments

On June 9, 2012, U.S. Cyber Command's General Keith Alexander announced that the NSA and the U.S. Cyber Command had also determined that the consensus guidelines are the path forward for protecting government and critical infrastructure computers and networks.

3 Introduction

In August 2012, the FCC indicated that it had recently become aware of the 20 Controls and convened Working Group 11 to determine the applicability of the 20 Controls to the communications sector. To effectively manage the effort, the FCC emphasized that the focus of this activity is on protection of carrier and ISP network operations both directly and through enterprise systems connected to operational technology; however, they did not include customer premises equipment. Working Group 11 was tasked with comparing the 20 Controls with the CSRIC II best practices and determining which of the CSRIC II best practices might need to be added to the 20 Controls to enable them to deal with the attacks frequently launched against communications companies and their infrastructure.

3.1 CSRIC Structure



3.2 CSRIC Working Group 11 Structure

Working Group 11 was co-chaired by Alan Paller of the SANS Institute and Marcus Sachs of Verizon Communications. Working Group 11 included representatives from user organizations, ISPs, suppliers of software and network equipment, academia, as well as other organizations that are a part of the Internet ecosystem.

3.3 Working Group 11 Team Members

Working Group 11 consists of the members listed below.

Name	Company
Doug Davis	Hypercube
Brett Kilbourne	Utilities Telecom Council
Jack Doane	Alabama State Government and NASCIO
Dan Traynor	Tennessee Valley Authority
Craig Spiezle	Online Trust Alliance
Dorothy Spears-Dean	VITA Virginia

Sue Plantz	California State Government
Mike O'Reirdan	MAAWG
Bill McInnis	Internet Identity
Patrick McGuire	California Office of Information Security
Micah Maciejewski	Sprint
Kevin Frank	Sprint
Frank Durda IV	Hypercube
Martin Dolly	AT&T
Tony Sager	National Security Agency (ret.)
Rodney Buie	TeleCommunications Systems
Ezra Berkenwald	Sprint
Robert Mayer	US Telecom
Andy Scott	NCTA
Chris Boyer	AT&T
Phil Agcaoili	Cox Communications
Russell Eubanks	Cox Communications
Allen Sautter	Cox Communications
David Dumas	Verizon
Jeffrey Barker	Syniverse Technologies
John Kelly	Comcast
Chris Richardson	Internet Identity
Michael Glenn	CenturyLink
Min Hyun	Microsoft
Beau Monday	Hawaiian Telcom

Table 1 - List of Working Group 11 Members

4 Objective, Scope, and Methodology

4.1 Objective

CSRIC tasked Working Group 11: Consensus Cyber Security Controls with determining the applicability of the consensus 20Controls to the communications sector, and with determining which existing CSRIC cyber security best practices should be included with the applicable critical controls to comprehensively cover known attack vectors – other than those attack vectors, such as Domain Name System (DNS) and Border Gateway Protocol (BGP), which were covered by other CSRIC III Working Groups.

4.2 Scope

This section identifies the problem statement, working group scope, and deliverables which were outlined in the CSRIC III working group description for Working Group 11.

Problem Statement: The growth of cyber security threats over the past decade has affected all parts of the Internet ecosystem, including the networks maintained by

communications providers. In particular, the rapid growth of advanced persistent threats (APTs), malware, and increasingly sophisticated and commercially available products represent a meaningful threat to the vitality and resiliency of the Internet and to the online economy. Communications providers and other ecosystem stakeholders and their government partners have a shared responsibility and mutual incentives to ensure the security and reliability of communication networks.

Working Group 11 Description: Working Group 11 was asked to examine and make recommendations to the Council regarding technical cyber security controls that can provide the most effective possible mitigation of known cyber risks to the systems and control elements that are likely to mitigate the risks of material and destructive consequences on provider networks and the customers they serve.

Working Group 11 was asked to "assess the degree to which the consensus lists of critical controls are applicable to the communications industry, identify gaps between the critical controls and the existing CSRIC best practices, and recommend a superset of the most critical controls for application in the communications industry. The Working Group will recommend updates to the best practices list."

DNS security, BGP security, and Botnet Remediation were out of scope for this effort because other CSRIC III working groups (Working Groups 5, 6, and 7 respectively) were tasked with addressing these critical Internet protocols.

4.3 Methodology

Working Group 11 began its research into practices that can mitigate cyber risks to carrier and ISP networks and operations by assembling a team of experts from multiple carrier and ISP segments, government, and academia, who collectively represent diverse stakeholders in the development and implementation of cyber risk mitigation practices and strategies. To accomplish this, Working Group 11 used several major work streams to accomplish the following:

(1) Analyze the 20 Controls for applicability to the communications industry.

(2) Analyze CSRIC II Working Group 2A: Cybersecurity Best Practices final report and recommendations, which included:

- Correlating all 397 best practices with the 20 Controls,
- Determining the uniqueness and applicability to the communications industry and challenges of implementation, and
- Determining which CSRIC 2A best practices should be classified as essential because they stop or mitigate damage from known attack vectors.

5 Recommendations

a. There is not a consensus within Working Group 11 regarding the extent to which the FCC should encourage the communications industry to use the 20 Controls. The

user community within Working Group 11 would prefer for the FCC to encourage industry to use the 20 Controls because they believe that the 20 Controls will protect the network infrastructure directly. The user group also believes that the 20 Controls have been demonstrated to be effective in protecting critical infrastructure from attacks that are likely to come through the enterprise systems and therefore the 20 Controls should be used by the communications industry. However, while the 20 Controls have been effective in guiding security management in enterprise and government institutions, the communications sector participants believe that some unique aspects of managing diverse multi-tenant communications networks will require additional evaluation in order to determine the extent to which the 20 Controls protect network infrastructure directly; as well as, to determine the applicability of the 20 Controls to communications sector.

b. The FCC should encourage the industry, working with experts from other areas of cyber security, to share threat information, to continue to define prioritized controls and to develop, prioritize, and refine associated best practices consistent with the ever evolving cyber-attacks and exploits.

c. The FCC should encourage continued review and improvement of cyber security practices for the communications sector to include:

a. Vetting the conclusions and recommendations of Working Group 11 by a broader cross-section of communications sector industry participants;
b. Updating, reorganizing, and prioritizing the cyber security best practices;
c. Estimating level-of-effort associated with typical implementations of such best practices;
d. Recommending technical cyber security controls that can provide the most effective possible mitigation of known cyber risks to the systems and control elements that are likely to mitigate the risks of material and destructive consequences on provider networks and the customers they serve;
e. Determining the extent to which the 20 Controls protect network infrastructure directly;
f. Determining the applicability of the 20 Controls to the communications sector;
g. Recommending a superset of the most critical controls that should be considered for application in the communications industry;
h. Determining the uniqueness and applicability to the communications industry and challenges of implementation;
i. Determining which CSRIC 2A best practices should be classified as essential because they stop or mitigate damage from known attack vectors;
j. Recommending the addition of a 21st Control, which is uniquely applicable to communications related to Distributed Denial of Service (DDoS) mitigation;
k. Assessing whether implementation of particular controls is applicable to communications or is likely to cause damage....."(and the related “notes” in Appendix 6, Task 1); and
l. Determining which of the best practices compiled by CSRIC II are important in stopping known attacks as outlined in Appendix 6, Task 4.

7 Conclusions

Working Group 11 evaluated the 20 Controls for their applicability to the Carrier and ISP network environment and found all 20 to be applicable in the environments they were designed to protect. It identified one critical control, applicable to all users of the Critical Controls, which was incomplete; and provided guidance to the 20 Critical Controls Steering Committee that was accepted for the upcoming version. It also found one major communications-specific control (DDoS mitigation) should be added to the 20 Controls, which would make it the 21 Critical Controls for Protecting Communications Infrastructure from Known Cyber Threats.

8 Appendices

Contents:

Appendix **1: The Assignment for Working Group 11**

Source: http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions.pdf

Working Group 11 – Consensus Cybersecurity Controls
Co-Chair – Alan Paller, SANS Institute
Co-Chair – Marcus Sachs, Verizon
FCC Liaison – Jeff Goldthorp

Description: This Working Group will examine and make recommendations to the Council regarding technical cybersecurity controls that can provide the most effective possible mitigation of known cyber risks to the business systems and networks maintained by communications providers and to the data maintained on and processed by those systems.

In carrying out its work, the working group will evaluate and contrast the "critical cyber security controls" adopted by the National Security Agency, the Department of Homeland Security in the United States, and the UK Centre for the Protection of National Infrastructure and the Australian Defense Signals Directorate, with the existing set of CSRIC cybersecurity best practices. The working group will assess the degree to which the consensus lists of critical controls are applicable to the communications industry, identify gaps between the critical controls and the existing CSRIC best practices, and recommend a superset of the most critical controls for application in the communications industry. The Working Group will recommend updates to the best practices list compiled by CSRIC II with a prioritized list of critical cybersecurity controls that are applicable to the communications industry.

Duration:
1. Revised, prioritized list of critical cybersecurity controls - March 6, 2013

Appendix 2: The FCC Liaison's Charge to the Working Group delivered by email to all members on August 30, 2012

Members of WG 11 -

Thank you for volunteering to contribute to WG 11. I would especially like to thank Alan Paller and Marc Sachs for agreeing to lead the work.

During the September 5 kick-off call, I will speak to the group about the charge the FCC has given the group. Alan will speak about the 20 Core Controls, including how they were arrived at. Marc will speak about the leadership's plans for the weeks ahead. We expect the meeting to be interactive.

I want to emphasize three things from the outset:

1. The focus of this activity is carrier and ISP network operations, which was the primary focus of the CSRIC II cybersecurity best practices. The Working Group will consider all CSRIC II Best Practices and compare them with the 20 Critical Controls.

2. The scope of this activity is the 20 Core Controls. I understand that there are subtending elements to the Controls and, to the extent the Working Group deems it helpful, we encourage them to be considered in the process. But this is not a requirement.

3. The CSRIC and its Working Groups are obligated to operate in full compliance with the Federal Advisory Committee Act. This statute places an emphasis on openness and transparency. Work product, including drafts, of WG 11, for example, is subject to public disclosure pursuant to the terms of the Freedom of Information Act (FOIA). The business of the Working Group should be conducted in an open fashion. Please keep this in mind as you conduct yourselves in the Working Group.

Thank you again for agreeing to support this important initiative,

Jeff Goldthorp
Designated Federal Officer
CSRIC

======

Appendix 3: The 20 Controls: a Brief History, the Controls, and Four Quick Wins

A Brief History of the 20 Critical Controls

In 2008, the Office of the Secretary of Defense asked the NSA for help in prioritizing the myriad security controls that were available for cybersecurity. The request went to the NSA because the NSA best understood how cyber attacks worked and which attacks were used most frequently. The request came at a moment when the theme "offense must inform defense" had become a White House mantra for cybersecurity.

The objective was to help DoD prioritize its cybersecurity spending. The NSA had been refining a list of security controls that were most effective in stopping known attacks since the early 2000s, which was based on earlier requests from the military services and reinforced by guidance from the White House. The Central Intelligence Agency's (CIA's) Tom Donahue, who was assigned to the White House cyber policy team, described the mandate as follows: "first fix the known bads." That meant no control should be made a priority unless it could be shown to stop or mitigate a known attack. That mandate was the key that came to separate the 20 critical controls from most other lists of controls.

The list of key controls that blocked the most frequent attacks was "for official use only" (FOUO) and could not be widely shared. However, the NSA had been participating in a public-private partnership involving the Center for Internet Security (CIS) and the SANS Institute for more than a decade. When approached by CIS and SANS, the NSA agreed to participate in a public-private consortium to share its attack information to provide the same type of control-prioritization knowledge for civilian government agencies and critical infrastructure. The NSA reasoned that the military could not protect the nation if the critical communications, power and financial sectors were not also protected.

The consortium members expanded to include others that had formal access to high value threat information, either because they had large teams that developed and used attack techniques or because they had large teams that performed the deep after-attack analysis that disclosed tactics, techniques and method used by attackers, Additions to the coalition included the United Kingdom's CESG (Communications-Electronics Security Group) and CPNI (Centre for Protection of Critical Infrastructure) the DoD, the FBI, as well as a number of companies in the incident response field, such as Mandiant and InGuardians, who did high value analysis of major attacks. Further expansion brought in the Defense Cyber Crime Center, three Department of Energy (DOE) laboratories, and companies like McAfee and Lockheed that had experience with major breaches.

The group built consensus at each step, surprising many by their willingness to share sensitive attack data. The two overarching factors that enabled active sharing was (1) the agreement that only actual attack information could be used to justify adding any controls, and (2) the membership was so impressive that participants knew that the

results would be authoritative and they wanted to be active contributors to something that could make a difference in protecting the nation. Surprisingly, the clear consensus of the consortium was that there were only 20 Critical Controls that addressed the most prevalent attacks found in government and industry. This then became the focus for an initial draft document. The draft of the 20 Critical Controls was circulated in early 2009 to several hundred IT and security organizations for further review and comment. Over 50 organizations commented on the draft. They overwhelmingly endorsed the concept of a focused set of controls and the selection of the 20 Critical Controls. These commenters also provided valuable "fine tuning" to the control descriptions.

The consortium reconnected with current and additional members every 6 to 12 months to ensure new attack information was reflected fully and that new techniques for mitigating old attacks were included. Other improvements to the 20 Critical Controls over time include measures by which organizations could know how well they had implemented the controls and a list of automated tools that have been validated (by thorough reference checks) to be effective in implementing the controls.

In the fall of 2008, the Center for Strategic and International Studies (CSIS) had convened a bipartisan panel, at the request two leading members of Congress, called the Commission on Cybersecurity for the 44th Presidency. The Commission's report made CSIS a respected source of guidance on cyber security. As a continuation of the Commission's work, it was natural for CSIS to become the first publisher of the 20 Critical Controls.

In 2009, the U.S. Department of State validated the consensus controls by determining whether the controls covered the 3,085 attacks it had experienced in 2009. In a presentation to the Intelligence Community, the State Department CISO reported remarkable alignment of the consensus controls and the State Department actual attacks. He also launched a program to implement automated capabilities to enforce the key controls and provide daily mitigation status information to every system administrator across 24 time zones in which the State Department operates. With a very rapid achievement of a more than 88% reduction in vulnerability-based risk across 85,000 systems, the State Department's program became a model for large government and private sector organizations. In December of 2011, DHS named the State Department CISO as the director of the National Cyber Security Division, with the mandate to bring about the same type and level of risk reduction across the government and the critical infrastructure as he had led at the State Department.

Also in December 2011, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) announced to United Kingdom government agencies and critical industries that the United Kingdom government would adopt the 20 Critical Controls as the framework for securing the critical infrastructure going forward. And in May of 2012, the Commander of the U.S. Cyber Command and Director of the NSA announced that he believed adoption of the 20 Critical Controls was a good foundation for effective cybersecurity, and that they are an excellent example of how public and private sector organizations can voluntarily come together to improve security. His endorsement was the result of the NSAs investment over the period of a year of some of its top talent vetting the 20 Critical Controls to be certain they reflected the actual risks faced by industrial and government systems.

In June 2012, the Idaho National Laboratory, home of the National Supervisory Control And Data Acquisition **(**SCADA) Test Bed, of the U.S. Department of Energy, completed a very favorable analysis of how the 20 Critical Controls applied in the electric sector as a first step in assessing the applicability of the controls to specific industrial sectors.

The Controls

Updated versions of the 20 Critical Controls are maintained at

http://www.sans.org/critical-security-controls/

The Critical Controls, ordered generally by importance (and hyperlinked to the master 20 Critical Controls document):

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Within each of the critical controls, sub-controls are grouped in four categories:

1) Quick wins on fundamental aspects of information security to help an organization rapidly improve its security stance without major procedural, architectural, or technical changes to its environment.

2) Visibility and attribution measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

3) Improved information security configuration and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

4) Advanced sub-controls that use new technologies that provide maximum security but are harder to deploy or more expensive than commoditized security solutions.

Four Quick Wins

Substantial evidence exists to demonstrate that four low-cost, low-impact "Quick Wins" are effective in blocking the vast majority of the targeted intrusions known as "Advanced Persistent Threat" that have been responsible for the loss of terabytes of sensitive military and commercial intellectual property. Those four quick wins, generally considered to be the highest-impact, lowest cost security controls to protect important information systems, include:[2]

1) White listing

2) Application patching within 48 hours of patch release[3]

3) System patching within 48 hours of patch release[4]

4) Reduction in the number of users with administrative privileges

[2] While there is widespread agreement that white listing, application and system patching and reducing the number of users with administration privileges are useful tools and recommended steps that should be evaluated by Communications Sector Participants, application and system patching within 48 hours may not be suitable for all network elements in every instance, in particular in the mobile environment, and white listing may be appropriate in certain instances but not in others. There is a need for individual companies who have differing network architectures to determine the feasibility of these recommendations within their networks.

[3] One industry participant noted that inside major infrastructure organizations the implementation should be worded: "Commence the application patching process within 48 hours of patch release" to fit it into scheduled maintenance windows.

[4] Ibid. "Commence the system patching process within 48 hours of patch release"

Appendix 4: Membership and Voluntary Assignments

Co-chairs

*Alan Paller, SANS Institute
Marc Sachs, Verizon Communications

Active members, sorted by employer name

(Voluntary assignments shown in parentheses are the CSRIC II best practice categories that our Working Group evaluated to determine how to improve the 20 Critical Controls and adapt them for use in the communications industry.)

Martin Dolly, AT&T
Chris Boyer, AT&T (Wireless)
Michael Glenn, Century Link (IP Services)
John Kelly, Comcast (Encryption)
Russell Eubanks, Cox Communications (Incident Response, Vulnerability Management, plus most other categories)
Phil Agcaoili, Cox Communications (All categories other than Network)
Allen Sautter, Cox Communications (Network)
Beau Monday, Hawaiian Telcom (Legacy Services)
Frank Durda IV, Hypercube (Network)
*Doug Davis, Hypercube (Network)
Chris Richardson, Internet Identity (Incident Response, People)
Bill McInnis, Internet Identity (IP Services)
Min Hyun, Microsoft (Identity Management)
Andy Scott, National Cable & Telecommunications Association
Kevin Stine, NIST (People)
Tony Sager, NSA- Division Director, VAO, recently retired
*Craig Spiezle, Online Trust Alliance
Sue Plantz, Public Safety Communications Office, State of California (Network)
Patrick McGuire, California Office of Information Security (Incident Response, Vulnerability Management)
Micah H. Maciejewski, Sprint (Wireless)
Kevin Frank, Sprint (Wireless)
Ezra Berkenwald, Sprint (Wireless)
*Jack Doane, State of Alabama and the National Association of State CIOs (Identity Management)
Jeffery Barker, Syniverse Technologies (Network)
Rodney Buie, TeleCommunication Systems (Wireless)
*Dan Traynor, Tennessee Valley Authority
Robert Mayer, U.S. Telecom
*Brett Kilbourne, Utilities Telecom Council
Nadya Bartol, Utilities Telecom Council
David Dumas, Verizon Communications (Network)
*Dorothy Spears-Dean, Virginia Information Technologies Agency (Encryption, Legacy Services)

*Members of the FCC's Communications Security, Reliability, and Interoperability Council

Appendix 5: Exclusions and Limitations in the Analysis

Early in its deliberations, Working Group 11 determined that its charter would be constrained as follows:

1. The Working Group would limit its analysis to ISP and carrier systems and exclude systems that were located at customer premises, even if those systems were owned by the ISP or carrier.

    a. The group acknowledges that end users CPE (even operator owned) do have issues and need their own independent review by a future working group from the perspective of their implementation and place in the network.

    b. Other "home/office" equipment needs review as well. As technology increases in the workplace the risks of security incidents also increase. A lot of small businesses are turning the Microsoft Lync, Asterisk or similar platforms to mitigate costs. These turnkey solutions targeted at the home or very small offices, have considerable risk to them to both the users and the public networks. A future working group too should examine this.

    c. Carriers and ISPs are constantly innovating; therefore care was taken (and should be taken in the future) not to accidentally dictate architecture or implementation directives. Such things stifle innovation that the communications ecosystem needs to survive and remain competitive. It is vital that this paper and any derivative works do not mandate any details but rather point out the best practices as the time of its publication knowing full well that these practices will be quickly deprecated as time moves and evolution continues.

2. The Working Group would not duplicate activities of other CSRIC III Working Groups, particularly the following:

    a. Working Group 4: Network Security: defined as "best practices to secure the Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of the Domain Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions"

    b. Working Group 5 – DNSSEC Implementation Practices for ISPs

    c. Working Group 6 – Secure BGP Deployment

    d. Working Group 7 – Botnet Remediation

3. With regard to "enterprise systems," Mr. Goldthorp's charge (See Appendix 2) said:

    "The focus of this activity is carrier and ISP network operations, which was the primary focus of the CSRIC II cybersecurity best practices."

The Working Group determined that unsecured enterprise systems are a principal attack vector through which ISP and carrier network operations are attacked because the latter are frequently connected to the former and have widely known and widely exploited vulnerabilities. This finding is consistent with the CSRIC II cybersecurity best practices many of which were targeted to protecting enterprise systems. Therefore, Working Group 11 operated under the assumption that effective protection of enterprise systems is a necessary ingredient of effective protection of network operations.

Appendix 6: Tasks of Working Group 11, and Results

The Working Group's mandate was defined by the FCC and is posted on the FCC website (*Source: http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions.pdf*

Tasks assigned to the Working Group

"The working group will evaluate and contrast the "critical cyber security controls" adopted by the National Security Agency, the Department of Homeland Security in the United States, and the UK Centre for the Protection of National Infrastructure and the Australian Defense Signals Directorate, with the existing set of CSRIC cybersecurity best practices." The working group will

Task 1: "assess the degree to which the consensus lists of critical controls are applicable to the communications industry,

Task 2: "identify gaps between the critical controls and the existing CSRIC best practices, and

Task 3: "recommend a superset of the most critical controls for application in the communications industry.

Task 4: "recommend updates to the best practices list compiled by CSRIC II with a prioritized list of critical cybersecurity controls that are applicable to the communications industry."

Results

Task 1: *Assess the degree to which the consensus lists of critical controls are applicable to the communications industry.*

During September 2012, the Working Group systematically reviewed the 20 Controls Version 4.0 posted at http://www.sans.org/critical-security-controls/. Each Control was reviewed by at least two members of the Working Group and some Controls were reviewed by three members. The results are shown in Table A6.1 below.

Table A6.1 Applicability of Critical Controls to the Communications Industry

Critical Control	Applicable in Communications Enterprise Networks	Likely to Cause Damage if Implemented
Critical Control 1: Inventory of Authorized and Unauthorized Devices	Yes	No
Critical Control 2: Inventory of Authorized and Unauthorized Software	Yes	No
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Yes (Note 6)	Possibly (Note 1)
Critical Control 4: Continuous Vulnerability Assessment and Remediation	Yes	Possibly (Notes 4 and 20)
Critical Control 5: Malware Defenses	Yes (Note 12)	No
Critical Control 6: Application Software Security	Yes	No
Critical Control 7: Wireless Device Control	Yes (Note 3)	No
Critical Control 8: Data Recovery Capability	Yes	No
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	Yes	No
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Yes	Possibly (Note 8)
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	Yes	Possibly (Note 11)
Critical Control 12: Controlled Use of Administrative Privileges	Yes	Possibly (Note 5)
Critical Control 13: Boundary Defense	Yes	No
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	Yes	No
Critical Control 15: Controlled Access Based on the Need to Know	Yes	No
Critical Control 16: Account Monitoring and Control	Yes	Possibly (Note 9)
Critical Control 17: Data Loss Prevention	Yes	No (Note 10)
Critical Control 18: Incident Response and Management	Yes	No
Critical Control 19: Secure Network Engineering	Yes	Possibly (Note 2)
Critical Control 20: Penetration Tests and Red Team Exercises	Yes	Possibly (Note 7)

Note 1: The challenge is in operational management of images. Before implementation, extensive testing is required to ensure compatibility with mission-critical applications. Secure configurations do change over time, so regression testing is required before updating, especially for systems like production servers.

Note 2: This has the potential for adverse consequences given both the forced interaction between elements that are under the control of the Telco and those that are not (being the external user). Further, a poorly designed, implemented, and managed network infrastructure could cause outages or other actual damages.

Note 3: Some members accurately indicated that “is not typically deployed in the

communications infrastructure" but since the Working Group mandate covers enterprise systems weaknesses as well as infrastructure weaknesses, and because wireless technology is widely used in the enterprise setting, the answer to this question was "Yes."

Note 4: We have seen where scanning software has disrupted some systems and had to either cease scanning those systems or work with the vendor to fix their equipment to allow scanning. Running any type of automated vulnerability scanning tools against all the communications networks/systems on a weekly or daily basis is not practical. Some Telco systems already have their automated diagnostics that are run regularly and traffic processing and billing take priority.

Note 5: Although this is basic blocking and tackling for security generalists, this is operationally difficult in a communications environment. The implementation, measurement, and testing outlined is complex to implement.

Note 6: To apply Critical Control 3 in the communications infrastructure, recommend that the title of #3 be changed to encompass all devices that can be accessed or administered directly or indirectly using any Internet communications Protocol, or more generically, any Remote Access method. Such a change will also require changes in the body of #3, and may affect other Critical Controls. The reason is "Because of the nature of the equipment found in a communications network and its unique position, a successful attack into these systems is able to cause far greater harm, in terms of:

> (1) Disruption and/or undesired re-direction of communications over a geographically large area of the country or world,
>
> (2) Loss of communication confidentiality, including data/voice eavesdropping and/or intercept/alteration/destruction of communication and records of those communications, both historical and current, and
>
> (3) Because of the higher number of peering points to other networks and the higher bandwidth carrier networks typically have, an outward-facing denial of service or other forms of attacks launched from within a compromised communications network can have considerable disruptive volume and speed.

In addition, to implement the sub-control of encouraging vendors to deliver systems with secure configurations built in, recommend contractual requirements be put forth by government agencies purchasing similar equipment. This could encourage vendors to address a long list of existing problems. (Why? "We also consistently find that virtually all vendors of [communications] equipment themselves are the cause of the most potential and real security threats involving their equipment. These problems [one common example: unchangeable logins and passwords] are embedded in the equipment design across all components and devices of a system.")

Note 7: Scanning processes can create a resource load on the network. They can also create an outage situation for the target device that is being scanned for vulnerabilities.

Generally, outage situations can occur if the target device is already near full capacity, if the device is running operating system software that is several iterations below current versions, or if the scanning engine is not sufficiently tested against non-production devices to remove specific vulnerability tests that can cause outages for the target device. There must be sufficient review and rigorous control of scanning process to prevent such outages. Thus, it may not be appropriate to perform scanning for all network elements. It would depend upon the network element as determined by the operator.

Note 8: A device may need a different configuration depending on the environment and services it needs to be performing. Defining a specific secure configuration may prevent a device from performing all of its services as intended. On the other hand, another member of the Working Group wrote: This is a critical control for carriers. Hardening of network elements is the first line of defense against compromise of network elements. In general, this hardening must be viewed in the three major planes of traffic going to or through network elements: data plane, control plane and management plane.

Note 9: The impact is the possibility of disabling a critical service.

Note 10: No. Undoubtedly, there will be an occasional file or website that is blocked, yet is business essential. These few outliers can be handled through a well publicized exception process.

Note 11: Implementing the control Limitation and Control of Network Ports, Protocols, and Services would extra work to enable new and needed Network Ports, Protocols, and Services. Implementing this control could make it inconvenient as having all of these available for use by anyone at any time. Outages could also occur during network scanning that specifically looks for available Network Ports, Protocols, and Services.

Note 12: The application of this control would be limited in the core communications network. This control is geared more for an Enterprise environment where you will find personal computing devices and end users. End user devices that access OSS networks and network elements can implement all of these controls. However, most communication elements will not support commercial anti-malware tools as they are proprietary operating systems and hardware.

Tasks 2 and 3: *Identify gaps between the critical controls and the existing CSRIC 2A best practices and recommend a superset of the most critical controls for application in the communications industry.*

Working Group 11 found substantial consistency between the CSRIC II best practices and the 20 Controls. The Working Group members were able to identify a direct correspondence between nearly every CSRIC II best practice that they felt stopped or mitigated damage from known attacks, and one of the 20 Critical Controls. In other words, most of the CSRIC II best practices that were critical were already reflected in the 20 Controls. However, two major exceptions were discovered in which critical CSRIC II best practices were not included in the 20 Critical Controls. One of those exceptions affects all industries and government agencies that choose to base their cyber security defenses on the 20 Controls; the other exception is primarily specific to the communications industry. Those exceptions are listed and described in the following two sections.

CSRIC II Best Practices applicable to all users of the 20 Controls

One CSRIC II best practice, entitled "Training for Security Staff," was based on NRIC 7-7-8100 (changed by CSRIC II) and NIST 800-53 Revision 3 control AT-3:

> *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.*

Somewhat surprisingly, the 20 Controls "Security Skills" (Control 9) control was silent on developing specific skills for security staff and had focused almost entirely on security awareness for general users. The CSRIC II best practice was strongly supported by the findings of the Secretary of Homeland Security's 2012 Task Force on Cyberskills (Table 1 on pages 7-9 of https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf) that identified 10 security roles that were "mission critical" and the DHS report specified the damage that is being incurred by organizations that have not ensured they had access to people with those mission-critical skills.

When the team responsible for updating the 20 Controls was informed of the missing skills element, the leaders immediately sought approval from the participating organizations. Without objection, the element was added as a sub-control of Critical Control 9, and will be part of Version 4.4 of the 20 Controls that will be released in March 2013.

CSRIC II Best Practices unique to the communications industry

The 20 Controls did not include several CSRIC II Best Practices that are essential for stopping or mitigating damage from attacks that take advantage of the communications infrastructure to carry out their attacks.

One of the most damaging attacks to a communications company is distributed denial of service (DDoS). CSRIC II best practices included a six DDoS related items that might be combined into a single Critical Control number 21 for Communications.

A recommended superset of the most critical controls for application in the communications industry

A superset of the 20 Controls recommended for consideration by communications companies might include:

1. The existing 20 Controls because they stop or mitigate damage from known attacks and the Working Group found that all of them applied to communications companies.
2. Adding security skills development best practices, covering the mission-critical security roles, as part of Control 9. This change is being made by the team that maintains currency of the 20 Controls.
3. Add a Communications Control 21: Protecting Against Distributed Denial of Service Attacks that is detailed in the DDoS-related best practices found in CSRIC II.

The superset might well be named: *21 Critical Security Controls for the Communication Industry*.

Task 4: *Recommend updates to the best practices list compiled by CSRIC II with a prioritized list of critical cyber security controls that are applicable to the communications industry.*

The following list includes best practices compiled by CSRIC II that are also determined by Working Group 11 in CSRIC III as important in stopping known attacks. Thus this list can complement the 20 Controls by showing specific steps that may be taken in implementing them. It should be considered a work in progress and subject to continuous updating just as the 20 Controls are regularly updated to reflect new threat data.

Category	NRIC VII Cross Reference (New/Changed/Unchanged/ Deleted)	CSRIC II Best Practice	CSRIC Reference/Comments
Wireless	New	**Wifi Policies:** Service Providers and Network Operators should establish and enforce 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	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	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	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	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	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	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	New	Femtocell Security: Equipment Suppliers should ensure enterprise Femtocell hardware shall be tamper-proof.	
Wireless	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	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	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	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	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	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	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	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	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	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.
IP Services	New	**Routing Integrity:** Service Providers and Network Operators should use IPv6 BOGON lists to filter un-assigned address blocks at Network boundaries.	
IP Services	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	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	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	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	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	New	**Packet Filtering:** Service Providers and Network Operators should proxy remote HTTP access to the VoIP perimeter firewalls.	DISA-VoIP0245
IP Services	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	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	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	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	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	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
Network	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	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	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	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
Network	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	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	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	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	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	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, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: March 2008
Network	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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.	
Network	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.	

Network	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	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	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	New	**Spam:** Network Operators should perform content analysis of In-bound e-mails.	Source: Anti-Spam Best Practices and Technical Guidelines
Network	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	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	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.
People	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	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	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	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	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	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	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	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).
Legacy Services	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	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	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	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	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 the minimum.	NIIF Guidelines for SS7 Security.
Legacy Services	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.	-
Identity Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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
Encryption	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	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	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	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	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	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
Vulnerability Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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 Management	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).
Vulnerability Management	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
Vulnerability Management	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
Vulnerability Management	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

Incident Response	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	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	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	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	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	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	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	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	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	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	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