



---

March 2011

Working Group 2A  
Cyber Security Best Practices

Final Report

## Table of Contents

1	Results in Brief.....	3
1.1	Executive Summary .....	3
2	Introduction .....	3
2.1	CSRIC Structure.....	4
2.2	Working Group 2A Team Members .....	4
3	Objective, Scope, and Methodology .....	5
3.1	Objective .....	5
3.2	Scope .....	6
3.3	Methodology .....	6
3.3.1	Methodology Overview .....	6
3.3.2	Sub-Team Organization .....	7
3.3.2	Sub-Team Approach .....	9
4	Background .....	10
5	Analysis, Findings and Recommendations .....	10
5.1	Analysis .....	10
5.2	Findings.....	12
5.3	Recommendations .....	12
6	Conclusions .....	18
7	Appendix A – CSRIC Working Group 2A Reference List.....	19

# 1 Results in Brief

## 1.1 Executive Summary

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

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

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

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

## 2 Introduction

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

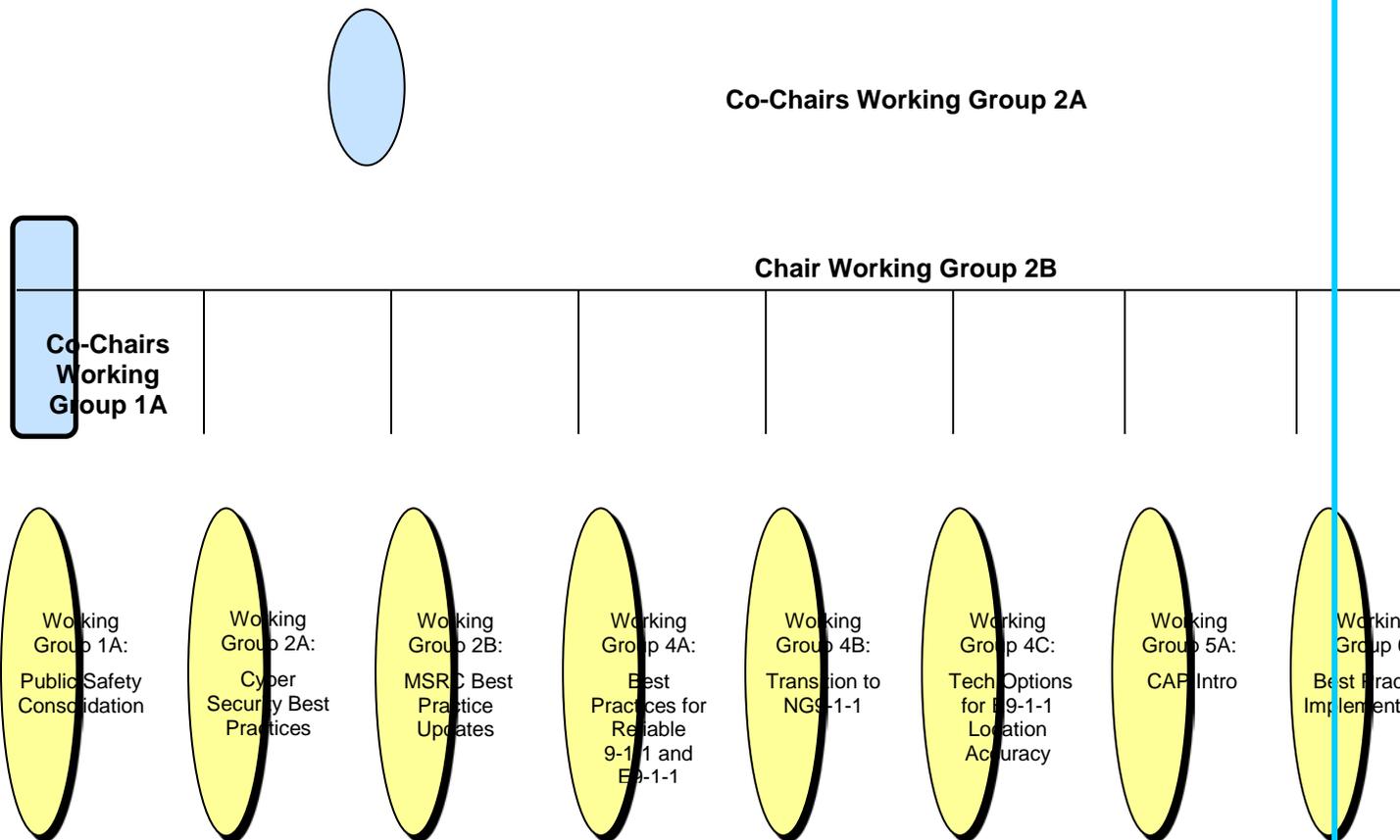
---

<sup>1</sup> CSRIC Working Group Descriptions Source: <http://www.fcc.gov/pshs/advisory/csric/wg-descriptions.pdf>

<sup>2</sup> Best Practice Tutorial Source: <http://www.bell-labs.com/USA/NRICbestpractices/tutorial.html>

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

## 2.1 CSRIC Structure



## 2.2 Working Group 2A Team Members

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

security. The FCC Liaison for Working Group 2A is Julia Tu.

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

Table 1 - List of Working Group Members

### 3 Objective, Scope, and Methodology

#### 3.1 Objective

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

## 3.2 Scope

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

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

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

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

## 3.3 Methodology

### 3.3.1 Methodology Overview

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

1. Voice over IP. "The focus group believes that future voice telecommunications will increasingly use this technology as network usage continues to converge between voice, video and data. This will include not only landline and broadband voice transmission, but also traditional wireless (e.g., cellular), voice, and data (e.g., wi-fi and WiMAX) networks.
2. Identity Management. "The need to correctly establish the authenticity of devices, humans and programs as they are used in network environments is becoming an increasingly critical issue."
3. Wireless security. "More and more endpoints in networking are migrating to a wireless environment whether via voice wireless networking or data wireless networking."
4. Blended attacks. "While basic definitions of what is a blended attack have been completed, the work of creating appropriate Best Practices to help deal with potential blended attacks is required." Blended attacks seeks to maximize the severity of damage

---

<sup>3</sup> NRIC VII FOCUS GROUP 2A Homeland Security Infrastructure Final Report  
[http://www.nric.org/meetings/docs/meeting\\_20051216/FG2B\\_Dec%2005\\_Final%20Report.pdf](http://www.nric.org/meetings/docs/meeting_20051216/FG2B_Dec%2005_Final%20Report.pdf)

by combining methods, for example using viruses and worms, while taking advantage of vulnerabilities in computers or networks.

5. Messaging security. “More and more operational components of networks are being managed by personnel who actively use various messaging products besides e-mail and voice communications.”
6. Utility computing. “As telecommunications use increases, companies strive to improve their computational delivery systems; there is a large push towards the use of utility computing platforms (blade servers, networked storage, virtual network connectivity and virtual security product implementations).”
7. Abuse Management. “In any area where technology is provided and where opportunists will attempt to take advantage of consumers and providers, there is the potential for fraud and abuse. While there are some Best Practices already provided that would start to help with the abuse problem, a great deal of additional work needs to be done to address the ever changing methods in which abuse and fraud are perpetrated on consumers and network providers.”
8. Strategic outlook for Best Practices. “One area the focus group recognizes is that current Best Practices are predominantly addressing operational networks and do not provide guidance or focus towards overall strategic issues in cyber security.”

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

### **3.3.2 Sub-Team Organization**

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

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

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

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

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

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

### 3.3.3 Sub-Group Approach

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

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

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

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

## 4 Background

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

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

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

## 5 Analysis, Findings and Recommendations

### 5.1 Analysis

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

#### 1. Wireless

---

<sup>4</sup> GAO Testimony before the Committee on Homeland Security, House of Representatives. CYBERSECURITY GAO-10-834T

<sup>5</sup> Poneman, Larry, “privacy breach Index Survey: Executive Summary”, Ponemon Institute, August 2008

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

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

## 5.2 Findings

### 1. Wireless

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

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

## **2. IP Services**

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

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

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

## **3. Network**

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

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

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

## **4. People**

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

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

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

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

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

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

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

## **5. Legacy Sub-Group**

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

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

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

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

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

## **6. Identity Management**

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

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

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

## **7. Encryption**

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

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

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

## **8. Vulnerability Management**

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

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

## **9. Incident Response**

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

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

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

### **5.3 Recommendations**

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

---

<sup>6</sup> Unknown, “The Financial Management of Cyber Risk: An Implementation Framework for CFOs”, Report pub. 2010 by the Internet Security Alliance, pp 39-46.

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

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

### **Service Provider Network Protection**

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

### **Border Gateway Protocol (BGP) Recommendation**

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

### **IP Television / Video on Demand**

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

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

## 6 Conclusions

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

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

---

<sup>7</sup> Wikipedia, <http://en.wikipedia.org/wiki/iptv>

## 7 Appendix A – CSRIC Working Group 2A Reference List

- "Hash Based IP Traceback" by Alex C Snoeren et.al of BBN published in Proceedings of the 2001 ACM SIBCOMM, San Diego, CA August 2001
- "Practical Network Support for IP Trace back" by Stefan Savage et.al., Dept. of Computer Science and Engineering, Univ of Washington, Tech Report UW-CSE-2000-02-01 with a version published in the Proceedings of the 2000 ACM SIBCOMM pp256-306 Stockholm, Sweden, August 2000
- "Satellite Security" Online Journal of Space Communication, number 6 (Winter 2004) <http://spacejournal.ohio.edu/issue6/main.html>
- 2009 Carnegie Mellon University, Author: Mindi McDowell posted on: <http://www.us-cert.gov/cas/tips/ST04-014.html>
- A physical network arrangement as described in "CENTERTRACK, An IP Overlay Network" by Robert Stone of UUNET presented at NANOG #17 October 5, 1999. John Ioannidis and Steven M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", NDSS, February 2002.
- American National Standards Institute (ANSI) X9.9, X9.52, X9.17
- Anti-Spam Framework of Best Practices and Technical Guidelines, National ICT Security and Emergency Response Center, 2005
- ATIS Packet Technologies and Systems Committee (previously part of T1S1)
- ATIS Protocol Interworking Committee (previously part of T1S1)
- ATIS-1000030, *Authentication and Authorization Requirements for Next Generation Network (NGN)*
- ATIS-1000035, *NGN Identity Management Framework*
- Carnegie-Mellon Software Engineering Institute secure software development: <http://www.sei.cmu.edu/engineering/engineering.html>
- Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, 3GPP, 3GPP2, LTE, etc.
- Center For Internet Security (CIS Benchmarks)
- Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
- COBIT: <http://www.isaca.org>
- Combating Spam – Best Practices – Sendmail Whitepaper – March 2007
- Committee on National Security Systems Policy (CNSSP) 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, 20 March 2007
- Common Criteria: <http://www.iso.org>
- Configuration guides for security from NIST (800-53 Rev. 3)
- Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 263-294.
- Defense information Systems Agency (DISA) - VoIP0210, VoIP0220, VoIP0230, VoIP0245, VoIP0270
- Department of Defense Telecommunications and Defense Switched Network Security Technical Implementation Guide (Version 2, Release 3)
- [doi.ieeeecomputersociety.org/10.1109/MSP.2008.8](http://doi.ieeeecomputersociety.org/10.1109/MSP.2008.8)
- draft-ietf-dhc-csr-07.txt, RFC 3397, RFC2132, RFC1536, RFC3118.
- Economic Espionage Act 1996

- Electronic Communications Privacy Act 1986
- Federal Information Processing Standards (FIPS) 140-2, PUB 46-3, PUB 74, PUB 81, PUB 171, PUB 180-1, PUB 197
- Garfinkel, Simson, and Gene Spafford. "Personnel Security". Practical UNIX & Internet Security, 2nd ed. Sebastopol, CA: O'Reilly and Associates, Inc. 1996. 389-395
- Garfinkel, Simson, and Gene Spafford. "Users, Groups, and the Superuser". Practical UNIX & Internet Security, 2nd ed. Sebastopol, CA: O'Reilly and Associates, Inc. 1996. 71-137
- Graham-Leach-Bliley Act 2002
- Guide to Security for WiMAX Technologies (Draft)
- Health Insurance Portability and Accountability Act (HIPAA) 2001
- <http://adsabs.harvard.edu/full/2004ESASP.558..243T>
- <http://blog.consumer-preference.com/2007/10/how-to-block-text-message-spam.html>
- <http://csrc.nist.gov>
- <http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf>
- <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>
- <http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf>
- <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-127>
- [http://en.wikipedia.org/wiki/E-mail\\_spam](http://en.wikipedia.org/wiki/E-mail_spam)
- [http://en.wikipedia.org/wiki/Mobile\\_phone\\_spam](http://en.wikipedia.org/wiki/Mobile_phone_spam)
- [http://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](http://en.wikipedia.org/wiki/Public_key_infrastructure)
- <http://ezinearticles.com/?Employee-Security-Awareness&id=4084497>
- <http://searchmobilecomputing.techtarget.com/tip/Best-practices-for-enterprise-mobile-device-and-smartphone-security>
- [http://searchsecurity.techtarget.com/tip/0,289483,sid14\\_gci1223151,00.html](http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1223151,00.html)
- <http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Sharon.htm>
- <http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-HackerTactics.html>
- <http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Dolan.html>
- <http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html>
- <http://spacejournal.ohio.edu/issue6/main.html>
- <http://spamlinks.net/prevent.htm>
- [http://ssmo\\_home.hst.nasa.gov/SSMO\\_Best\\_Practices\\_010705/best%20practices.htm](http://ssmo_home.hst.nasa.gov/SSMO_Best_Practices_010705/best%20practices.htm)
- <http://standards.ieee.org/getieee802/download/802.11w-2009.pdf>
- [http://wapedia.mobi/en/3GPP\\_Long\\_Term\\_Evolution](http://wapedia.mobi/en/3GPP_Long_Term_Evolution)
- <http://www.3gpp.org/ftp/Specs/html-info/21133.htm>
- <http://www.aiaa.org/images/spaceops/SOSTC-BestPractices.pdf>
- [http://www.airspan.com/pdfs/WP\\_Mobile\\_WiMAX\\_Security.pdf](http://www.airspan.com/pdfs/WP_Mobile_WiMAX_Security.pdf)
- [http://www.alertboot.com/blog/blogs/endpoint\\_security/archive/2010/06/15/laptop-encryption-software-for-social-security-administration-telecommuters.aspx](http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/06/15/laptop-encryption-software-for-social-security-administration-telecommuters.aspx)
- [http://www.amazon.com/Hacking-Exposed-5th-Stuart-McClure/dp/B0018SYWW0/ref=sr\\_1\\_1?ie=UTF8&s=books&qid=1251593453&sr=1-1](http://www.amazon.com/Hacking-Exposed-5th-Stuart-McClure/dp/B0018SYWW0/ref=sr_1_1?ie=UTF8&s=books&qid=1251593453&sr=1-1)
- <http://www.atis.org/> - ATIS-0300276.2008 Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane: March 2008

- <http://www.atstake.com/services/smartrisk/application.html>
- [http://www.ca.com/files/whitepapers/data-loss-prevention-requirements-wp\\_203570.pdf](http://www.ca.com/files/whitepapers/data-loss-prevention-requirements-wp_203570.pdf)
- <http://www.csoonline.com/article/596163/mobile-phone-security-dos-and-don-ts?page=1>
- <http://www.cybercrime.gov>
- [http://www.cybersecurity.my/data/content\\_files/13/65.pdf?.diff=1176418561](http://www.cybersecurity.my/data/content_files/13/65.pdf?.diff=1176418561)
- <http://www.cymru.com/Bogons/index.html>, NSTAC ISP Working Group - BGP/DNS, RIPE-181, "A Route-Filtering Model for Improving Global Internet Routing Robustness" [222.iops.org/Documents/routing.html](http://222.iops.org/Documents/routing.html)
- NIST SP 800-54 Border Gateway Protocol Security
- <http://www.enisa.europa.eu/act/it/eid/mobile-eid>
- <http://www.fedcirc.gov/homeusers/HomeComputerSecurity/> Industry standard tools (e.g., LC4).
- <http://www.gao.gov/new.items/d02781.pdf>
- [http://www.georgia.gov/vgn/images/portal/cit\\_1210/0/26/99359541Enterprise%20Information%20Security%20Charter%20PS-08-005.01.pdf](http://www.georgia.gov/vgn/images/portal/cit_1210/0/26/99359541Enterprise%20Information%20Security%20Charter%20PS-08-005.01.pdf)
- <http://www.ietf.org/rfc/rfc1321.txt>
- <http://www.ietf.org/rfc/rfc3882.txt>
- [http://www.imation.com/smb/laptop\\_data\\_protect.html](http://www.imation.com/smb/laptop_data_protect.html)
- [http://www.inmarsat.com/Downloads/English/FleetBroadband/Getting\\_started/FleetBroadband\\_Best\\_Practices\\_Manual.pdf?language=EN&textonly=False](http://www.inmarsat.com/Downloads/English/FleetBroadband/Getting_started/FleetBroadband_Best_Practices_Manual.pdf?language=EN&textonly=False)
- <http://www.k-state.edu/its/security/procedures/mobile.html>
- [http://www.linuxmagic.com/opensource/anti\\_spam/bestpractices](http://www.linuxmagic.com/opensource/anti_spam/bestpractices)
- <http://www.microsoft.com/atwork/security/laptopsecurity.aspx>
- [http://www.rsa.com/products/DLP/wp/8738\\_PEDL\\_WP\\_0409.pdf](http://www.rsa.com/products/DLP/wp/8738_PEDL_WP_0409.pdf)
- <http://www.sans.org>
- <http://www.scps.org/>
- <http://www.securityforum.org>
- <http://www.securityinnovation.com/pdf/security-awareness-best-practices.pdf>
- [http://www.sendmail.com/sm/wp/spam\\_best\\_practices/](http://www.sendmail.com/sm/wp/spam_best_practices/)
- <http://www.social-engineer.org/Newsletter/SocialEngineerNewsletterVol02Is07.htm>
- <http://www.sophos.com/security/best-practice/spam.html>
- <http://www.stonybrook.edu/nyssecure>
- <http://www.us-cert.gov/cas/tips/ST04-014.html>
- <http://www.usshortcodeswhois.com/>
- [http://www.windowsecurity.com/articles/Social\\_Engineers.html](http://www.windowsecurity.com/articles/Social_Engineers.html)
- <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm>
- [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)
- Information Security Forum. "Security Audit/Review". The Forum's Standard of Good Practice, The Standard for Information Security. November 2000.
- International Organization for Standardization (ISO) 17799, 27002
- International Telecommunication Union (ITU) - CCITT Rec. X.700 (X.720) Series, Rec. X.800 Series, SS7 Standards, "Securing SS7 Telecommunications Networks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 5-6 June 2001, Rec. X.805, Rec. X.812, Rec. X.815, Rec. X.1051, X.1250, *Baseline capabilities for enhanced global identity management and interoperability*, Y.2702,

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

- Internet Engineering Task Force (IETF) RFC 2547, RFC 3813 & draft-ietf-l3vpn-security-framework-02.txt, RFC 2350, rfc3013 section 3, 4.3 and 4.4, RFC 3227, RFC 4942, RFC-1034, RFC-1035, RFC-2065, RFC-2181, RFC-2535, RFC-2870
- Internet Systems Consortium (ISC) BIND 9.2.1 US-CERT "Securing an Internet Name Server" (<http://www.cert.org/archive/pdf/dns.pdf>)
- ISP Resources. [www.IATF.net](http://www.IATF.net)
- King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. "Applying Policies to Derive the Requirements". Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 66-110
- King, Christopher M., Curtis E. Dalton, and T. Ertem Osmanoglu. "Platform Hardening". Security Architecture, Design, Deployment & Operations. Berkley, CA: The McGraw-Hill Companies. 2001. 256-284
- Liberty Alliance Project, Privacy and Security Best Practices Version 2.0
- McClure, Stuart, Joel Scambray, George Kurtz. "Dial-Up, PBX, Voicemail, and VPN Hacking". Hacking Exposed, Network Security Secrets and Solutions, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 341-389.
- McClure, Stuart, Joel Scambray, George Kurtz. "Enumeration". Hacking Exposed, Network Security Secrets and Solutions, 4th Edition. Berkley, CA. The McGraw-Hill Companies. 2003. 69-124.
- MPLS Forum interoperability testing (<http://www.mplsforum.org>).
- National Institute of Standards and Technology. "Access Control Mechanisms, Access Control Lists (ACLs)". Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996; "Secure Authentication Data as it is Entered". Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996
- National Security Agency (NSA) Security Configuration Guides; VOIP and IP Telephony Security Configuration Guides
- National Security Telecommunications advisory Committee (NSTAC) ISP Working Group - BGP/DNS
- Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Access Controls - Two Views". Defending Your Digital Assets Against Hackers, Crackers, Spies and Thieves. New York, NY. The McGraw-Hill Companies. 2000. 242-261
- Nichols, Randall K., Daniel J. Ryan, Julie J. C. H. Ryan. "Digital Signatures and Certification Authorities - Technology, Policy, and Legal Issues".
- NIIF Guidelines for SS7 Security.
- NIST 800-53 revision 3: Recommended Security Controls for Federal Information Systems and Organizations security control catalogue; NIST IR-7622, DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems; NIST SP 800-115 A Technical Guide to Information Security Testing and Assessment; NIST SP 800-119 (Draft) 2.4, (Draft) 3.5.6, (Draft) 3.6.2, (Draft) 4.2.3, (Draft) 6.5.2; NIST SP 800-40 v2.0 Creating a Patch and Vulnerability Management Program Dependency on NRIC BP 8034 and 8035; NIST SP 800-54 Border Gateway Protocol Security; NIST SP 800-63, *Electronic Authentication Guideline*; NIST SP 800-81 & SP 800-81 R1 Secure Domain Name System(DNS) Deployment Guide; NIST SP800-118 Guide to Enterprise

Password Management <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>; NIST SP800-14 Generally accepted principles and practices for securing IT systems. <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>; NIST SP800-57 Recommendation for key management [http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2\\_Mar08-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf); NIST SP800-83 Guide to malware incident prevention and handling; <http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>; NIST SP800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>; NIST Special Pub 800-12, Pub 800-14, Pub 800-26; NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*; NIST Special Publication 800-53, Revision 3, Control Number PM-7 Recommended Security Controls for Federal Information Systems [http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated-errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf); NIST: [www.nist.gov](http://www.nist.gov) Document is SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003; SP800-45 (NIST) <http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf> Guidelines on Electronic Mail Security

- North American Network Operators Group (NANOG) (<http://www.nanog.org>)
- Octave Catalog of Practices, Version 2.0, CMU/SEI-2001- TR-20 (<http://www.cert.org/archive/pdf/01tr020.pdf>)
- Office of Management and Budget (OMB) Circular A-130 Appendix III.
- Organization for the Advancement of Structured Information Standards (OASIS), Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0
- PacketCable Security 2.0 Technical Report (PKT-TR-SEC-V05-080425); Security Specification PKT-SP-SEC-I11-040730, IETF RFC 3261
- RIPE-181, "A Route-Filtering Model for Improving Global Internet Routing Robustness" [www.iops.org/Documents/routing.html](http://www.iops.org/Documents/routing.html)
- Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 8 - 14.
- Sarbanes-Oxley 2003
- Schneier, Bruce. 1996. Applied Cryptography. 2d.ed. John Wiley & Sons.
- Secure Programming Educational Material at <http://www.cerias.purdue.edu/homes/pmeunier/secprog/sanitized/>
- Space Communications Protocol Standards (SCPS) Including ISO Standards 15891:2000 through 15894:2000 and related documents <http://www.scps.org/>
- Stopping Spam – Report of the Task Force on Spam – May 2005IS
- [technet.microsoft.com/en-us/library/cc875806.aspx](http://technet.microsoft.com/en-us/library/cc875806.aspx)
- Telcordia GR-815. Cellular Standards: GSM, PCS2000, CDMA, 1XRTT, UMTS, etc.
- Telecommunications Act 1996
- US Government and National Security Telecommunications Advisory Committee (NSTAC) Network Security Information Exchange (NSIE). "Administration of Static Passwords and User Ids". Operations, Administration, Maintenance, & Provisioning (OAM&P) Security Requirements for Public Telecommunications Network. Draft 2.0, August 2002.

- US Government and National Security Telecommunications Advisory Committee (NSTAC) ISP Network Operations Working Group. "Short Term Recommendations". Report of the ISP Working Group for Network Operations/Administration. May 1, 2002.
- USA PATRIOT Act 2002
- US-CERT "Securing an Internet Name Server"
- [www.cert.org/archive/pdf/CSInotes.pdf](http://www.cert.org/archive/pdf/CSInotes.pdf)
- [www.cert.org/archive/pdf/defcappellimoore0804.pdf](http://www.cert.org/archive/pdf/defcappellimoore0804.pdf)
- [www.cert.org/security-improvement/practices/p072.html](http://www.cert.org/security-improvement/practices/p072.html)
- [www.cert.org/security-improvement/practices/p096.html](http://www.cert.org/security-improvement/practices/p096.html)
- [www.cio.ca.gov/OIS/Government/documents/ppt/insider-threat.ppt](http://www.cio.ca.gov/OIS/Government/documents/ppt/insider-threat.ppt)
- [www.sans.org/reading\\_room/.../logrhythm-monitoring-may-2010.pdf](http://www.sans.org/reading_room/.../logrhythm-monitoring-may-2010.pdf)
- [www.state.nj.us/it/ps/](http://www.state.nj.us/it/ps/)
- [www.us-cert.gov/GFIRST/abstracts.html](http://www.us-cert.gov/GFIRST/abstracts.html)