NRIC VII

December, 2005

FOCUS GROUP 2B

Summary of Activities, Guidance and Cybersecurity Issues

Table of Contents

1 Introduction

1.1 Purpose of Document

This document provides a summary of work completed by NRIC focus group 2B (Cybersecurity) from January, 2004, through December, 2005. It also provides guidance information for future focus group activities as well as findings by the focus group requiring attention by the FCC.

1.2 Composition of Focus Group

The NRIC FG2B (cybersecurity) focus group was comprised of technically qualified cyber security representatives from NRIC member companies as well as selected subject matter experts in specific areas of cyber security from industry and a few Federal agencies. Additionally, large enterprise organizations and companies that provide critical technology components to the membership provided cyber security expertise to help develop the cyber security Best Practices. Focus group members averaged well over 10 years of individual technical cyber security experience and most focus group members are direct practitioners of cyber security at their company. Most focus group members had also achieved at least one industry standard personal security certification such as being a certified information systems security professional (CISSP), certified information security manager (CISM) or certified information security auditor (CISA), which are each ANSI and ISO certified and recognized security credentials.

1.3 Who should implement NRIC FG2B (Cybersecurity) Best Practices?

While the main focus of NRIC Best Practices are for telecommunications sector companies, the cyber security focus group, from its inception, has recognized that large and small enterprise companies as well as technology vendors may find that the Best Practices provided are not only practical but can be implemented across a wide range of company types. Not all Best Practices will apply to all companies nor are there Best Practices for all situations in which a company may find a cyber security problem. In situations where another focus group may have developed a useful cyber security Best Practice, it may have been included in the list of cyber security Best Practices with the source of the Best Practice listed in the reference section of the provided Best Practice. It was the goal of the focus group to provide a highly useful, practical set of cyber security Best Practices that meet the highest industry standards irrelevant of the source. If a source for a Best Practice was accidentally omitted, please accept our apologies and notify the FG2B chairman so that the proper reference can be made.

2 Summary of Activities

The charter of focus group 2B required the focus group to review all previously created cyber security Best Practices from all previous NRICs, make adjustments where necessary to update the Best Practices, add additional new Best Practices where required, and work with other focus groups to eliminate duplicate Best Practices if found or add new ones as recommended by other focus groups. The focus group completed the review and update of all previously generated cyber security Best Practices by December 2004, and delivered the reviewed and completed set of Best Practices to the NRIC Council. This effort was accomplished approximately one year ahead of schedule. It was recommended to the Council that future focus groups perform this review at least every two years to ensure that Best Practices are continually current and up-to-date. Also, the update ensures that NRIC member organizations following the Best Practices are not confused by multiple sets of cyber security Best Practices for which implementation dates may be confusing. In this manner, companies desiring to implement a wide range of the Best Practices can retrieve the latest updated set without having to search through many previous incarnations and determine which Best Practices are current and valid. In addition to a thorough review of the existing Best Practices from NRIC I through NRIC VI, the focus group also worked with other focus groups to eliminate duplication of Best Practices as well as incorporate cyber security topics that were brought up by other focus groups. Continuing from work established in NRIC VI, the focus group worked closely with FG2A to establish specific definitions for blended attacks as a baseline to work from to create future Best Practices for blended attacks. Basically, a blended attack is where physical attacks (such as a truck bomb) against a specific asset (such as a power grid control center) are combined with a cyber space attack (such as a router table attack against a power grid management system) to more thoroughly disable an asset and cause massive harm. Additional work was started on the issue of cyber security for technologies such as identity management, voice over IP, and wireless security for data and voice networks. The focus group also worked closely with other focus groups to review and comment on documents and deliverables produced by the various focus groups under the charter for NRIC VII. This included work on first responder/emergency services and networking, broadband, public data networks, infrastructure, and wireless issues.

3 Recommended Guidance for Future Focus Group Activities in Cyber Security

NRIC VII Focus Group 2B recommends that future cyber security focus groups consider work in the following areas:

- 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. Voice over IP is very different than traditional SS7 voice transmission methods and requires different security mechanisms than have been traditionally used in SS7 network environments. Focus Group 2B is especially concerned about cyber security and reliability issues of the IP protocol when used in emergency services/first responder networks of all types.

- 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. Not only is identity management critical for traditional management plane activities and technologies, it is also becoming a critical component to fight the proliferation of malware such as worms and address spoofing attacks which lead to distributed denial of service conditions on networks. Historically, identity management has been largely implemented as password control systems and in some cases token or biometric access methods for a very limited range of technologies. The focus group believes that near-term technologies will require additional focus on a variety of identification techniques as well as establishment of “trusted broker” methods to convey identification technologies between networks, applications and companies. The issues of identity management and cyber security will rapidly become a network management problem as operating system vendors deploy new versions of their operating environments, which will require a variety of two factor authentication. The focus group also believes that legislation pending in the United States will force companies to adopt much stronger identity management technologies to be compliant with the expected legislation. The adoption of stronger identity management technologies will cause increased member company capital and operational expenditures to satisfy required compliance.

- Wireless security (licensed and unlicensed). More and more endpoints in networking are migrating to a wireless environment whether via voice wireless networking or data wireless networking. While significant work has happened over last five years in wireless security controls, the focus group believes that a significant amount of additional work will need to be done to provide for proper security of wireless networks.

- 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. This will be a complex undertaking that will require significant thought and modeling to create effective Best Practices and recommendations.

- 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. Additionally, many devices from handsets to network components are being delivered with built-in messaging options that are not part of the historical methods used to intercommunicate. Best Practices that provide for security of messaging technologies as well as secure message content need to be identified and developed. Messaging in its various forms is rapidly becoming a staple not only for consumers but also for teams managing network operations.

- 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). Best Practices need to be identified, thought out, and recommendations established for the cyber security needs of utility computing and how it is used to deliver services, as well as how it is used in the management plane of network operations.

- 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. Items such as phishing attacks, fraudulent messaging, zombie and bot nets, interoperability of abuse investigations in management between carriers and many other related items will need Best Practice development as the technologies are changed and new technologies are introduced into use.

- 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. The focus group believes that additional Best Practice work needs to be undertaken to provide for a more strategic view of cyber security topics to get ahead of potential attacks and to provide a more balanced security investment model by member companies.

4 Issues and Concerns Outside of Best Practices for NRIC and the FCC to Consider

The following section highlights items that the focus group considers to be important to address, which are probably inappropriate for Best Practices. The focus group presents these items as significant issues that need to be addressed in the area of cyber security. As experts in the technical merits of cyber security issues, the focus group believes these items to be of major concern, which need to be addressed at a national level or the cyber security problems around these issues will increase in severity.

1. Upgrade of TCP/IP and associated protocol suites to include cyber security features. In NRIC VI, the cyber security focus group recommended that basic and fundamental research be funded and undertaken to provide a “heavy lift” of the TCP/IP protocol suite and associated protocols to improve the reliability of the protocols as well as provide for reasonable security controls. The focus group believes that many security problems currently encountered will become much worse as the protocols are used more and more to deliver services to the consumer base. The focus group also believes that many security problems currently experienced could be eliminated if the various protocols used in the TCP/IP protocol suite had security controls implemented within the protocols. This is a problem which is rapidly expanding as the protocol usage of TCP/IP explodes. Unless some basic controls are provided within the protocol suites, the focus group believes that many security problems experienced on networks using TCP/IP protocol suites will continue to reflect a band-aid security effort by companies attempting to implement security cheaply or haphazardly on networks running TCP/IP protocol suites. While some of the protocols

that are used within the TCP/IP suite contain reasonable security controls, the bulk of the protocols used do not. Further, some protocols such as DNSsec and secure BGP are so difficult to upgrade and so onerous to implement that they remain largely unimplemented because of the difficulties they present in transitioning to the new, more secure protocols. Further, the focus group does not believe that IPv6 effectively solves the security problems that are constantly present on IP networks. The focus group believes that the implementations of IPv6 will be as problematic in security concerns as IPv4 and will introduce new security problems not yet envisioned. In fact, hybrid IPv4/IPv6 networks increase the complexity of the network and may introduce new vulnerabilities. Some layers of the protocol suite, such as IP itself, do not implement any security controls and are easily violated. The focus group believes that it will take several years for a proper upgrade of the TCP/IP suite to be engineered, developed and deployed. We do not believe that this work is being reasonably organized and properly funded so that a successful outcome (a secure TCP/IP network suite) can be achieved. As more and more critical applications are deployed on an unsecured TCP/IP protocol suite, the risk for outages, hack attacks and other sorts of malfeasance are certain. One suggested path forward may be to establish a focus group under NRIC VIII which is dedicated to the problem of identifying research topics of concern to cyber security in the TCP/IP protocol suites. The focus group places a very high priority on this activity due to the continued an aggressive deployment of TCP/IP as the preferred transport protocol for critical infrastructure, such as emergency/first responder networks and infrastructure.

2. Confidential cyber security Best Practices. The focus group finds many areas where Best Practices might be implemented but the creation of such a Best Practice would easily lead the opposition into a realization of how they might attack critical infrastructure - successfully so. There needs to be a mechanism by which teams, such as the cyber security focus group, can create sensitive Best Practices which will be useful for companies that provide network and application services and yet such sensitive Best Practices would not be available to the nefarious opposition. While the focus group realizes the benefit of publication of Best Practices for cyber security to the general public, there is a subset of Best Practices that could be developed which would require a high level of confidentiality so that implementers could mitigate the potential risk, put in safeguards to deal with the vulnerability and yet not have that vulnerability highlighted for opposing parties, (i.e., the threat). The very nature of NRIC's public disclosure requirements negates the ability for the focus group to develop these sensitive Best Practices, which are very useful when implemented

but would unnecessarily expose the industry to attacks and threats by malicious opposition. As an example, the focus group knows of specific critical infrastructure networking assets which are highly vulnerable to a blended attack. If a set of Best Practices was developed to deal with the specific types of blended attacks, it would be relatively easy for a malicious opposition group to read the Best Practice and determine that a specific critical infrastructure is vulnerable and the type of attack to launch. The focus group believes that predicting all possible combinations of blended attack scenarios was not possible/worthwhile and preventative Best Practices for single vectors combined with communication and correlation Best Practices for blended attacks would be more useful.

3. Improved confidential sharing of threat information. While it is outside the scope of the NRIC FG2B charter and scope of mission, the membership of the focus group is increasingly frustrated with the lack of sharing of useful, and most likely confidential, cyber security threat vector information available to the United States government. Most of the membership actively participates in the telecommunications ISAC and have for many years. Increasingly, the focus group membership believes that confidential threat information is not making it to the membership where it can be applied toward securing of critical infrastructure. The focus group believes that the FCC and DHS need to be more aggressive in promulgating sensitive threat information to the focus group membership to allow the membership take an active role in protecting of critical resources. How and what shape this interaction needs to take is unknown at this writing. The focus group does believe, however, that some effort needs to be put forth to figure out a safe and secure method by which confidential threat and vulnerability information can be shared not only from the government but among NRIC membership. The focus group proposes three specific items to consider: 1) Federal government share more (specific) classified and unclassified threat information with the telecommunications industry 2) an improved inter-company incident/outage analysis function be created (possibly within the National Communication Center) and 3) that such analysis should feed an improved threat information dissemination process.

5 Appendix: Attachments

Please see the attached file entitled “FG 2B_Final Best Practices_December 2005” containing proposed changes to the cyber security Best Practices that have already been approved by the Council.