

NRIC VII

December 6, 2004

FOCUS GROUP 2B

Homeland Security
Cyber Security Best Practices

Report #1

Table of Contents

1. Results in Brief
2. Introduction
 - 2.1. Structure of NRIC VII
 - 2.2. Focus Group 2B Team Members
3. Background
4. Objective, Scope, and Methodology
 - 4.1. Objective
 - 4.2. Scope
 - 4.3. Methodology
5. Analysis and Findings
6. Next Steps
7. Appendices
 - 7.1. Appendix X: Computer Security Incident Response Process
 - 7.2. Appendix Y: Responding to New or Unrecognized Anomalous Events
 - 7.3. Appendix Z: Incident Response Post Mortem Checklist

1 Results in Brief

A total of 173 existing NRIC Best Practices related to Cyber Security were reviewed to determine if changes were required to these best practices or to determine if gaps existed between NRIC Best Practices and existing industry Best Practices for Cyber Security. The results were as follows:

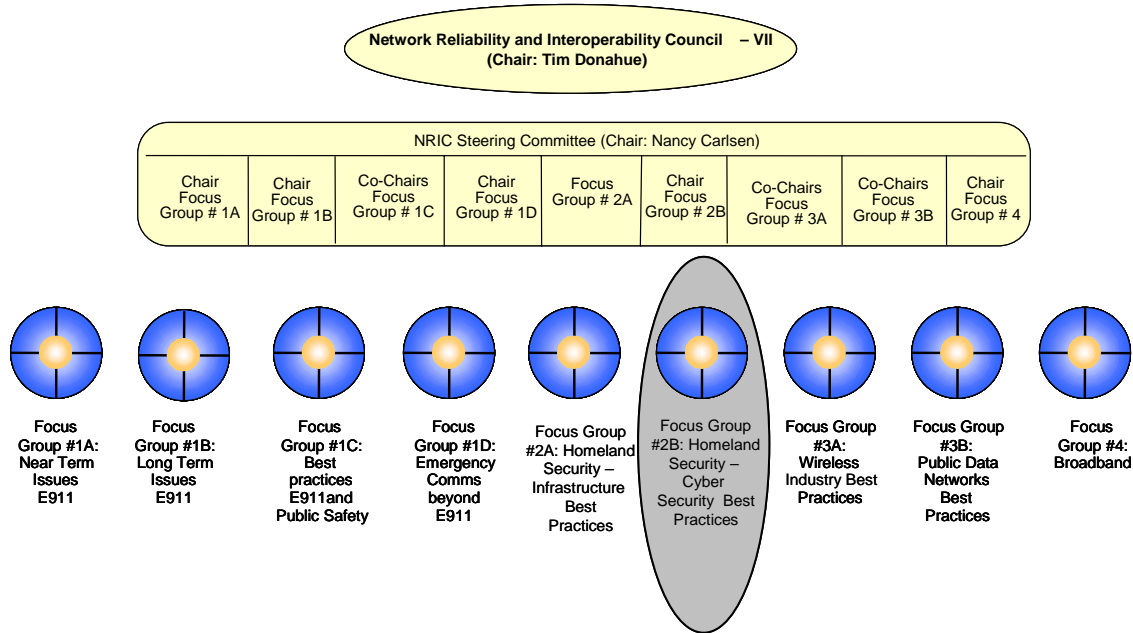
- 111 Best Practices were updated to incorporate new data in the area of each Best Practice
- 14 Best Practices were recommended for deletion as they are superseded by other existing NRIC Best Practices
- 48 Best Practices were left unchanged
- 28 new Best Practices currently being used by industry were added

2 Introduction

This report documents the efforts undertaken by the Network Reliability and Interoperability Council (NRIC) VII Focus Group 2B with respect to the review and updating of Cyber Security Best Practices.

2.1 Structure of NRIC VII

The structure of the Network Reliability and Interoperability Council is as follows:



2.2 Focus Group 2B Team Members

Focus Group 2B consists of 37 members. The group was broken into five subgroups to focus on the following areas: Scrubbing existing Best Practices, VoIP, Blended Attacks, Abuse and Utility Computing. Additionally, liaisons to each of the other NRIC Focus Groups were appointed to ensure coordination.

Focus Group 2B Members

Name	Company
Brennan Baybeck	Qwest
Matt Broda	Nortel
Ken Buckley	Federal Reserve Board
Dorian Deane	MCI Communications
Victor DeVito	AT&T
Vinnit Duggal	Intelsat
Brian Estep	Alltel
Bob Fairbairn	Motorola
Jerry Freese	AEP
Chris Guttman McCabe	CTIA
Dr. Bill Hancock - Chair	
Chris Harris	Verizon Wireless
Jeff Hartley	Cox Communications
Frank Horsfall	Nortel Networks
Richard Hovey	Federal Communications Commission
Daniel C. Hurley, Jr.	Dept. of Commerce
Bill Jaeger	AT&T
Gregory C. Jensen	SAFLINK Corporation
Bruce Kaalund	Comcast IP Services
Alan H. Komenski	Bellevue Police Dept (WA)
Rosemary Leffler	SBC Communications
Theresa Menzel	MCI Communications
Rick Myers	Syniverse
Shannon Myers	Savvis Communications
Jose Peña	Nextel
Dr. Mark Petrovic	Earthlink
John Rittinghouse	Rittinghouse Consulting LLC
Jim Runyon	Lucent
Richard Salgado	Department of Justice
Satwik Seshasai	MIT
Greg Shannon	System Detection, Inc
Randy Shannon	CenturyTel
John Stogoski	Sprint
Bob Thornberry	Lucent
Rick Waddell	Microsoft
Rod Wallace	Nortel Networks
Michael White	Nextel

3 Background

The Network Reliability and Interoperability Council was originally established to study the causes of service outages and to develop recommendations to reduce their number and their effects on consumers.¹ NRIC's I-IV concentrated on reliability concerns in a number of areas including signaling (SS7), fiber cuts, switching systems, power failures, fires, 911 outages, and digital cross-connect systems, with little focus on Cyber Security.

The Homeland Defense Group was chartered by NRIC VI in March 2002 to focus on the development of Best Practices to prevent disruptions of public telecommunications services and the Internet and to effectively restore those services in the case of disruptions. This Focus Group delivered 151 Cyber Security Best Practices to the NRIC VI Council.

NRIC VII Focus Group 2B will use these Cyber Security Best Practices developed during NRIC VI as a base, and will update and expand on those as necessary.

4 Objective, Scope, and Methodology

4.1 Objective

The NRIC VII Council has been charged with reviewing and improving the Homeland Security Best Practices that were adopted by the NRIC VI Council. The NRIC VII Charter states:

“By December 16, 2005, the Council shall present a final report that describes, in detail, any additions, deletions, or modifications that should be made to the Homeland Security Best Practices that were adopted by the preceding Council.”²

In an effort to provide appropriate focus on both Infrastructure and Cyber Security Best Practices, two Focus Groups were assigned to this objective. Focus Group 2A is looking at the Infrastructure Best Practices, and Focus Group 2B is reviewing the Cyber Security Best Practices.

4.2 Scope

The scope of this document is limited to Cyber Security Best Practices and does not address Infrastructure Best Practices.

¹ www.nric.org

² NRIC VII Charter, www.nric.org

This report contains the following:

- Analysis of existing NRIC Best Practices related to Cyber Security
- Recommended additions, deletions and modifications to those existing Best Practices
- Identification of new Cyber Security Best Practices

Future deliverables for Focus Group 2B will include additional new Cyber Security Best Practices, especially in the areas of wireless and VoIP, as well as a glossary of Cyber Security terms.

4.3 Methodology

Following is the methodology that Focus Group 2B followed to develop this report:

- 1) A threat/vulnerability analysis was done FIRST to identify Best Practice requirements
- 2) Industry sources were surveyed to determine if a Best Practice already existed elsewhere
- 3) A Gap Analysis was done to identify areas where a threat or vulnerability exists and for which there is no known Best Practice in existence
- 4) Best Practice requirements were "grouped" into subject matter general categories (like VoIP, blended attacks, patching, etc.)
- 5) Teams of experts worked on generating Best Practices based upon their skill set and experience, and adhered to the following guidelines:
 - Best Practices are short and focus on WHAT, not "how" something is done
 - A Best Practice must be implementable (the team knows it can be done or it has been done by one or more of the team membership)
 - A Best Practice must be practical and make sense (nothing theoretical or hypothetical)
 - Best Practice "language" must follow Chicago Book of Style
- 6) Best Practice drafts were circulated to the entire focus group and the responsible team made any changes
- 7) All focus group members met to achieve consensus on all Best Practices that were put forward to Council
- 8) Final edits were made to the Best Practices
- 9) Best Practices were formatted for inclusion into the website database and are numbered accordingly

5 Analysis and Findings

The attached file entitled "NRICVII_FG2B_December2004_BPs_Appendices.pdf" contains the Best Practices that were reviewed along with a recommendation for each Best Practice (Change, Delete, Add, Unchanged). Additional comments and references are included for many of the Best Practices as well.

6 Next Steps

With the completion of the review of existing Cyber Security Best Practices, the next step for Focus Group 2B will be to continue with the generation of new Best Practices, especially in the areas of wireless and VoIP. The team intends to create a glossary of Cyber Security terms to provide a better understanding of terms used in the Best Practices. The team is also considering developing a conformance and measurement section so that the Best Practices may be evaluated for implementation purposes.

7 Appendices

7.1 Appendix X: Computer Security Incident Response Process

See attached file entitled "NRICVII_FG2B_December2004_BPs_Appendices.pdf"

7.2 Appendix Y: Responding to New or Unrecognized Anomalous Events

See attached file entitled "NRICVII_FG2B_December2004_BPs_Appendices.pdf"

7.3 Appendix Z: Incident Response Post Mortem Checklist

See attached file entitled "NRICVII_FG2B_December2004_BPs_Appendices.pdf"