NRIC

Network Reliability and Interoperability Council

FG2B

Cybersecurity

Dr. Bill Hancock, CISSP, CISM

SAVVIS Communications

FG2B Chair

bill.hancock@savvis.net

972-740-7347

Purpose of Today's Brief

- **Brief discussion of work completed per NRIC VII mission statement**
- **Formal request for approval of NRIC VII FG2B Cybersecurity BPs**
- **Notice of ongoing and future work**

FG2B Mission Statement

“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.”

Base FG2B Mission Completed

- **A complete review of all cybersecurity-related Best Practices from NRIC I through NRIC VII**
- **202 BPs submitted for Council approval with three text appendices on incident response (appendices X, Y and Z)**
- **Some BPs were:**
  - **Split for clarity**
  - **Added where needed**
  - **Deleted obsolete BPs**
- **FG2B created one, current master set of BPs from all NRICs**

How FG2B Accomplished its Deliverables

- **FG2B divided into teams aligned along working methods at NRIC membership:**
  - **Security Architecture: Bill Jaeger (AT&T)**
  - **Security Engineering: Bill Jaeger (AT&T)**
  - **Security Administration: Greg Jensen (Saflink)**
  - **Security Operations: Ron Mathis (Intrado)**
  - **Policy Compliance & Awareness: Tim Bowe (Sprint) and Chris Harris (Verizon)**
  - **Application Development: Greg Jensen (Saflink)**
- **"Scrub" team coordination by Dan Hurley of US Department of Commerce**

Work Methodology for “Scrub”

- **Painstakingly review each cybersecurity BP for all NRICs by qualified, experienced, credentialed cybersecurity experts:**
  - **Completeness**
  - **Correctness**
  - **Relevancy to current issues/environments**
- **Review of external standards, BPs or other documents from other orgs that support, negate or enhance BPs created**
- **Consensus review by entire FG2B team**
- **Internal NRIC membership review(s)**

Formal Request for Approval of FG2B Best Practices

- **Complete review of all cybersecurity BPs from all NRIC sessions**
- **Approval and acceptance of 202 cybersecurity BPs that supersede all previous publications of cybersecurity BPs of all NRICs**
- **This creates one, current master set of cybersecurity BPs for NRIC members to implement**
- **It is recommended that NRIC perform this function in all future NRICs so that ONE master set of updated cybrsecurity BPs are available for each future NRIC effort to reduce confusion and guarantee relevance to the mission**

Special “Thank You” to…

- **To the team leaders, of course, and…**
  - **Bob Thornberry (Lucent) and Bill Jaeger (AT&T) for their extraordinary effort, especially toward the end of the effort, in getting the deliverable finished**
- **In addition, the following team members contributed helpful analyses and input at critical times:**
  - **Dorian Deane (MCI)**
  - **Bob Holley (Cisco)**
  - **Frank Horsfall (NortelNetworks)**
  - **Vanessa Pegueros (AT&T Wireless)**
  - **Michael White (Nextel)**

What's Next at FG2B?

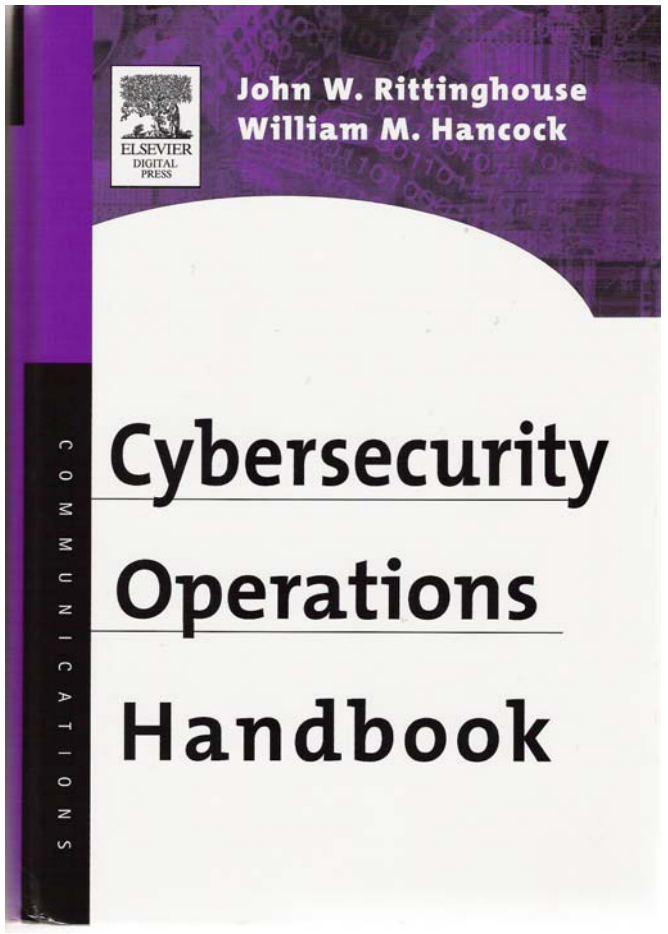
- **Continued coordination and support to all other NRIC FGs in cybersecurity**
- **Creation of new BPs in:**
  - **Blended attack issues**
  - **VoIP**
  - **Wireless networks**
  - **Public data networks**
  - **Utility computing environments**
  - **Broadband networks**
- **Execution criteria for FG2B cybersecurity BPs**

BPs and Implementation Guidance

Number	6-6-8008
Title	Network Architecture Isolation/Partitioning
Preventative Best Practice	**Compartmentalization of technical assets is a basic isolation principle of security where contamination or damage to one part of an overall asset chain does not disrupt or destroy other parts of an asset chain. Network Operators and Service Providers should give deliberate thought to and document an Architecture plan that partitions and isolates network communities and information, through the use of firewalls, DMZ or (virtual) private networks. In particular, where feasible, it is suggested the user traffic networks, network management infrastructure network, customer transaction system networks and enterprise communication/business operations networks be separated and partitioned from one another. Special care must to taken to assess OS, protocol and application vulnerabilities, and subsequently hardened and secure systems and applications, which are located in DMZ's or exposed to the open Internet.**
Reference	**ISF SB52, www.sans.org**
Dependency	
Implementor	**NO, SP**

202 BPs FG2B

+



1300 pages

Continued Areas of Concern

- **Major concerns still exist for:**
  - **Heavy-lift security upgrade of traditional protocols and methods**
    - **Many highly popular protocols subject to many types of simplistic attacks due to lack of security controls and methods in the protocols themselves**
  - **ASN.1**
  - **Promoting NRIC cybersecurity BPs by the FCC to US government network teams to protect such networks and infrastructure**

NRIC VII FG2B Outreach

- Communications event participation
- Speeches and gatherings
- White papers
- NRIC web site
- Many others…

NRIC

Network Reliability and Interoperability Council

Questions?

Dr. Bill Hancock, CISSP, CISM
SAVVIS Communications
FG2B Chair
bill.hancock@savvis.net
972-740-7347