NRIC

Network Reliability and Interoperability Council

# NRIC Best Practices for ISP Security

# Agenda

- **Overview of the Network Reliability and Interoperability Council (NRIC)**
- **NRIC Best Practices for Security**
- **Next steps**

NRIC
Network Reliability and Interoperability Council

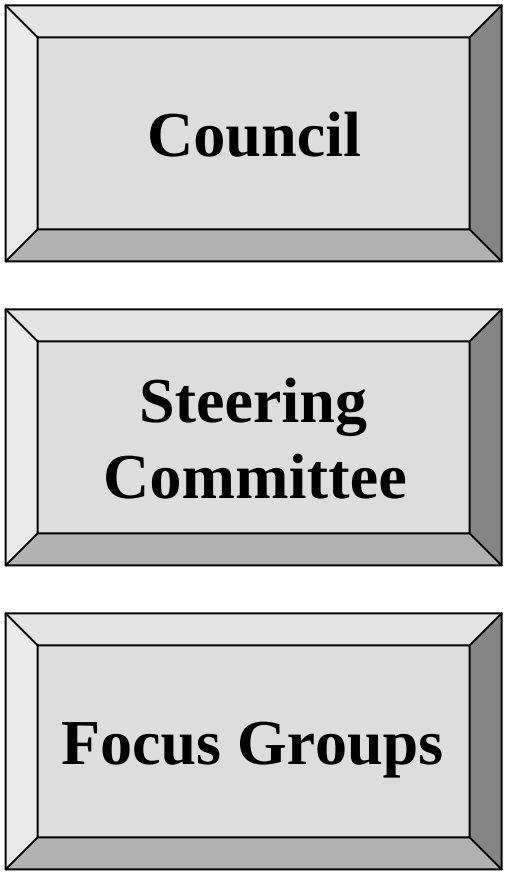
# What Is NRIC?

- **A Federal Advisory Committee chartered by the FCC**
  - **Extensive participation by service providers and vendors**
- **Originally chartered in 1992 in the wake of major service outages**
- **Develops industry Best Practices to promote network reliability and interoperability**

# How Is NRIC VI Different?

- **Extension of charter to address external threats**
  - **Establish Best Practices for security**
- **Participation from a much wider variety of industry segments.**
  - **Carrier, CATV, Wireless, ISP, Equipment Supplier, Systems Integrator**
- **CEO-Level representation on Council**

# NRIC VI Structure




Chaired by Richard Notebaert
CEO Qwest

Chaired by Pam Stegora Axberg
Sr VP Reliability Qwest

Subject Matter Experts

# NRIC VI Focus Group Structure

**Focus Group 1 Homeland Security**

A. Physical Security (K.Rauscher, **Lucent Technologies**)
B. Cyber Security (Bill Hancock, **Cable & Wireless**)
C. Public Safety (M.Roden / D.Dautel, **Cingular / Motorola**)
D. Disaster Recovery & Mutual Aid
(J.Tumolo / G.Barber, **Verizon / BellSouth**)

**Focus Group 2 Network Reliability**

(P.J.Aduskevicz, **AT&T**
R.Callon, **Juniper**
W.Hall, **Comcast**)

**Focus Group 3 Network Interoperability**

(C.Naughton**, Boeing**)

**Focus Group 4 Broadband**

(D.Davis**, Allegiance)**

# Agenda

- Overview of NRIC
- **NRIC Best Practices for Security**
  - **Principles for Best Practices**
  - **Focus Group 1B, Cybersecurity**
- Next Steps

NRIC
Network Reliability and Interoperability Council

# History: NRIC BPs for Reliability

- **BPs provide guidance on ways to improve network reliability**
  - Implementation is optional
  - Confirmation of effectiveness based on review of actual outages
- **Fifth Council Survey Results**
  - Risk to not implement the BPs
  - Not a high cost to implement BPs
  - BPs are effective in preventing outages
  - Already a high level of implementation

# Principles in Developing BPs

1. ***People*** **implement best practices**
2. **Do *not endorse* commercial or special "pay for" documents**
3. **Address *classes* of problems**
4. ***Already implemented***
   **(not always appropriate for cyber security)**
5. **Developed by *industry consensus***
6. **Best Practices are verified by a *broad set* of industry members**
7. **Sufficient *rigor* and *deliberation***

# Current Work on Best Practices

- **Physical Security**
- **Cyber Security**
- **Public Safety**
- **Disaster Recovery and Mutual Aid**

NRIC

Network Reliability and Interoperability Council

# Focus Group 1B
# Cybersecurity

**Dr. Bill Hancock, CISSP, CISM**

**Cable & Wireless**

**FG1B Chair**

**bill.hancock@cw.com**

# Charter of FG1B

- Generate Best Practices for cybersecurity
  - Telecommunications sector
  - Internet services
- Propose New Actions (if needed)
- Deliverables
  - December 2002 – prevention (105 BPs)
  - March 2003 – recovery (45 BPs)

# Some “Slammer” Lessons

- **Rapid propagation time**
  - **Code Red in 2001 took many hours (self replication in 37 minutes on average)**
  - **Slammer estimates are 8.5 seconds**
- **Worm was very small and efficient**
  - **Payload was NIL, but easily could have been very, very UGLY**
- **Companies that followed appropriate FG1B BPs *a priori* were *unaffected* by Slammer**

# Applicable FG1B Prevention Best Practices

**6-6-8000 Disable Unnecessary Services**
**6-6-8008 Network Architecture Isolation/Partitioning**
**6-6-8015 Segmenting Management Domains**
**6-6-8020 Security HyperPatching**
**6-6-8032 Patching Practices**
**6-6-8034 Software Patching Policy**
**6-6-8037 System Inventory Maintenance**
**6-6-8039 Patch/Fix Verification**
**6-6-8041 Prevent Network Element Resource Saturation**
**6-6-8071 Threat Awareness**
**6-6-8074 Denial of Service Attack – Target**
**6-6-8093 Validate source addresses**

# Example of a Best Practice

**6-6-8000: Service Providers and Network Operators should disable unneeded network-accessible services that are not needed or used on any network/service element or management system when practical (e.g., Network Time Protocol (NTP), Remote Procedure Calls (RPC), Finger, Rsh-type commands, etc.).**

# What Does this Mean to NRIC?

- **Prevention of cyberattack  is cheaper**
  - **Maintain reliability, SLAs**
  - **Reduce manpower costs**
  - **Consistent service and delivery**
  - **Increase customer satisfaction**
  - **Reduce support costs**
  - **Reduce negative PR burden**
  - **Many others…**
- **Investment in security is important**

# Agenda

- Overview of NRIC
- NRIC Best Practices for Security
- **Next Steps**

NRIC
Network Reliability and Interoperability Council

# Next Steps

- **Look at the best practices for physical and cyber security**
- **Deploy best practices**
  - **Where appropriate**
  - **To prevent or mitigate future attacks**
- **Optionally, participate in NRIC efforts**
  - **Such as updates to best practices**

# Intended Use of Best Practices

- **Provides guidance on how best to protect the U.S. communications infrastructure**
- **Implementation is voluntary**
- **Service Providers, Network Operators, and Equipment Suppliers are urged to prioritize**
- **Decisions of whether or not to implement a specific Best Practice are left with the responsible organization**

# Information on BPs

- **Best Practices main page**

  **http://www.bell-labs.com/user/krauscher/nric/**

  **(or go to www.nric.org; click on best practices)**
- **Physical Security BPs**

  **http://www.bell-labs.com/cgi-user/krauscher/action.pl?Submit=Submit&physical_security=1**
- **Cybersecurity BPs**

  **http://www.bell-labs.com/cgi-user/krauscher/action.pl?Submit=Submit&cyber_security=1**

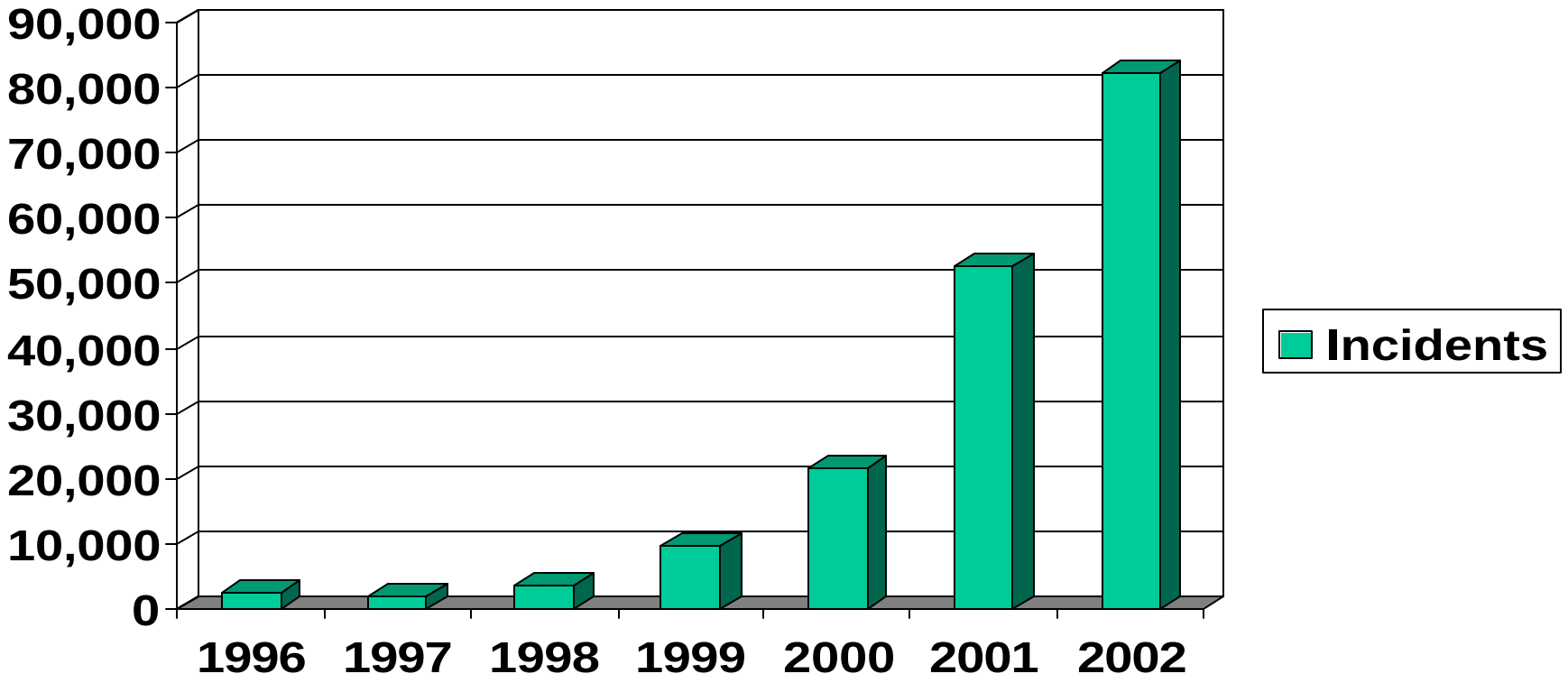
# Information on NRIC

- Web site: www.nric.org
- Pamela Stegora Axberg

  Chair – NRIC VI Steering Committee
  pstegor@qwest.com
- Jeffery Goldthorp

  Designated Federal Officer – NRIC VI
  jgoldtho@fcc.gov

# Summary: A Call to Action




**Source: CERT/CC (www.cert.org)**