
NATIONAL INFRASTRUCTURE
NIAC
ADVISORY COUNCIL

NIAC Vulnerability Disclosure Working Group

Status Report & Update

The North American Network Operators' Group (NANOG28)

2003 June 02

Organization

- **National Infrastructure Advisory Council**
  - **Advises the President of the United States regarding the security of information systems supporting critical infrastructure sectors**
  - **Composed of CEOs or equivalent from the private sector, academia, and state and local government (but not US Federal Government)**

NIAC Working Groups

- Focus on specific topics (such as vulnerability disclosure)
- Can engage in fact-finding, research, or seek input
- Cannot participate in lobbying nor advise Congress
- Cannot comment on any actual working group output without approval from the NIAC

Why Are We Here Today?

- Because we “Can engage in fact-finding, research, or seek input”
- This is just an overview
- Get the full story at the BoF session later
- Tell us what you think; we need your feedback

VDWG Mission & Scope

- **Guidelines for handling a security vulnerability from initial report to final resolution**
- **Audience includes government, education, private industry, the public, and other stakeholders**
- **Builds on existing best practices and wide range of experience from working group members and others**
- **Derive specific recommendations for the President and the US Federal Government from those guidelines**

Background

- Vulnerability reports continue to increase
- Great diversity of practice, goals, and values among those who handle vulnerabilities
- The Internet is global, but stakeholders have obligations to their own constituencies
- NIAC charged by Executive Order to provide recommendations which will improve sharing between ISACs, DHS, and other agencies

Working Group Members

- **Co-Chairs:**
  - **John Chambers, Cisco Systems**
  - **John Thompson, Symantec**
- **Participants include ISS, Mitre, CERT/CC, Verizon, Counterpane, Fannie Mae, UC Davis, Microsoft, IT-ISAC, Telecom-ISAC, FS-ISAC, ISC, DHS/IAIP**

Problem Definition

- **How does one share information about a vulnerability with the appropriate parties without compromising others or the critical infrastructure?**
- **How do the participants become aware of all of the considerations so as to make the best decisions, possibly in an emergency?**
- **What does full disclosure mean? What are its variations?**

Initial Input for Content

- **Vulnerability disclosure practices from working group members**
- **CERT/CC Vulnerability Questionnaire**
- **Other submitted industry best practices**
- **Various contributing research papers, articles, and case studies**

In Agreement

- **The Internet has no physical boundaries; thus consideration has to be global but with an obvious focus on national constituents.**
- **Limit working group activity to vulnerability disclosure.**
- **Those with a plan survive; write it down now**
- **Industry agrees it can and will solve this problem, and is aware of the urgency.**

In Consensus

- No “One size fits all”; focus on processes to
  - Avoid surprises, and
  - Make decisions with complete awareness
- Similar efforts do not directly overlap
  - OIS, INCH (IETF), FIRST Vendor Group
- Consider varying missions and constituencies
  - Manufacturers and vendors of products and services
  - Consultants who provide warnings to customers
  - Coordinating agencies for the common good
  - Other critical infrastructure sectors

Timeline

- Group has been meeting since March
- External review in late May and June
- Final version submitted for executive approval afterwards with submission to the next NIAC meeting to follow (currently expected in mid-July)
- Schedule may be adjusted depending on feedback and workload

Deliverables

- **Full report expected by 2003 June 30**
- **Various status reports in the interim, including presentations to other groups during external review**
- **More information is solicited, but the authors have enough information to begin writing the basic framework**

Comments and Suggestions

- **Principal authors:**
  - **Adam Rak, Symantec**
  - **Jim Duncan, Cisco Systems**
- **Additional contacts:**
  - **Rob Clyde, Symantec**
  - **Ken Watson, Cisco Systems**
- **E-mail:**
  - **niac-vdwg@external.cisco.com**

Your Feedback Requested!

- More to follow at the ISP Security BoF III tonight
- Other questions during NANOG28? Please contact:
  - Jim Duncan, jnduncan@cisco.com
  - Paul Vixie, paul@vix.com
- After NANOG28?
  - niac-vdwg@external.cisco.com


NATIONAL INFRASTRUCTURE
NIAC
ADVISORY COUNCIL