PANEL STATEMENT

Nontechnical Issues in Achieving Dependably Secure Systems and Networks

National Information Systems Security Conference,
Crystal City, Virginia, 18-21 October 1999

Chairman:
Peter G. Neumann, Computer Science Lab, SRI International, Menlo Park CA

Panelists:
George Dinolt <George.W.Dinolt@lmco.com>, Lockheed Martin

Virgil Gligor <Gligor@eng.umd.edu>, Department of Electrical Engineering, University of Maryland, College Park MD

Sami Saydjari <SSaydjari@DARPA.mil>, DARPA

Brian Snow <Bsnow@radium.ncsc.mil>, NSA

This panel will consider the realistic challenges of achieving dependably secure systems and networks, including perspectives of computer science education, software engineering, criteria, formal methods, multilevel security, government funding, market forces, and the open-source movement. Rather than being a hodge-podge of unrelated ideas, the intent of the panel is to see if we can integrate all of these perspectives into a unified whole that is much greater than the sum of its parts. What lessons must be learned from our past experience, and what must we do differently in the future?

In our eternal quest for system and network security, the NISS Conference has tended to focus on system development, evaluation, procurement, operation, and use. The proposed panel seeks to transcend those issues, and to consider some of the many obstacles impeding that quest—from a broader perspective. Illustrative questions to be discussed might include a subset of some of the following:

- What should our universities be teaching to increase the understanding of software development and dependably secure systems?
- What about training computer system administrators and system development managers?
- What are realistic expectations of software engineering disciplines in developing secure systems?
- What could the computer industry do differently that would be effective, within their needs for economic competitiveness?
- What R&D directions are not being adequately pursued that might realistically have a constructive effect on commercial systems and on government deployments?
- What can governments do differently that would encourage the availability of systems and networks with greater security?
- Are there relevant lessons that we should learn from the Y2K fiasco?
- What hope do we have for establishing criteria that meaningfully constrain security and that can be extensively fulfilled?

- Can the open-source, free software, and nonproprietary movements lead to systems that are dramatically more robust than commercial systems?
- Could serious liability laws constrain developers and purveyors of systems that engender huge losses or cause critical failures?
- To what extent are our critical national infrastructures affected by a lack of robust systems and networks?

BACKGROUND FOR INTENDED AUDIENCE:

This is a big-picture session that seeks to get to the roots of many of the problems confronting us all, and to consider how those problems might relate to one another. It is intended for EVERYONE, and cuts across many disciplines and many special interests. It should be useful for people involved in requirements, criteria, architecture, system design, implementation, security, survivable systems, system procurement, software engineering, education, etc.

Peter G. Neumann
SRI International EL-243
333 Ravenswood Avenue
Menlo Park CA 94025-3493
Telephone 1-650-859-2375

Fax 650-859-2844

Neumann@CSL.sri.com