NISSC PANEL PROPOSAL

PANEL DISCUSSION: Critical Infrastructure Assurance

ABSTRACT: Presidential Decision Directive 63 (PDD-63) has ordered the strengthening of the nation's defenses against emerging unconventional threats to the United States to include those involving terrorist acts, weapons of mass destruction, assaults on our critical infrastructures and cyber-based attacks. The panel will discuss the events subsequent to the signing of Presidential Decision Directive on Critical Infrastructure Protection (PDD-63) and the activities of various Federal department and agencies as called for in the First Annual National Plan for Information Systems Protection.

- Overview of PDD-63 — Mr. Davis
- National Information Infrastructure Assurance Plan — Mr. Tritak
- Federal Sector Coordination — Mr. Burke
- Research and Development — Mr. Davis
- Private Sector Outreach — Ms. Wong
- Legal Initiatives — Mr. Mitchell

CHAIR: John Tritak, Director, Critical Infrastructure Assurance Office

PANELISTS: Thomas Burke, General Services Administration
Stevan Mitchell, Department of Justice
John Davis, National Security Agency
Nancy Wong, Pacific Gas and Electric

POINT OF CONTACT: Charmayne Parks
Office of Information Security
Federal Technology Service
General Services Administration
(202) 708-5623
charmayne.parks@gsa.gov

Stevan D. Mitchell, Trial Attorney
Computer Crime and Intellectual Property Section
U.S. Department of Justice
(202) 514-1026
stevan.mitchell@usdoj.gov

NISSC POSITION STATEMENT

The President's Commission on Critical Infrastructure Protection (PCCIP) identified information sharing as "the most immediate need" for the development of enhanced infrastructure assurance. The PCCIP called for "the creation of a trusted environment that would allow the government and the private sector to share sensitive information openly and voluntarily," and recognized that "[s]uccess [would] depend on the ability to protect as well as disseminate needed information." Its objective was to facilitate the flow of information three ways: among government entities; among private-sector entities, and between government and the private sector. To accomplish this, the Commission recommended creation of various information-sharing structures within government and the private sector, and also identified a number of potential legal "impediments" to information sharing.

These legal impediments were abstracted from extensive discussions with industry about barriers, real or perceived, that appeared to discourage sharing of sensitive information, including:

- *Liability issues*: Parties, including governmental entities, may be reluctant to share sensitive information if doing so would subject them to additional liability risk.

- *Antitrust issues*. Private sector entities may be reluctant to share sensitive threat and vulnerability information with one another if by so doing they face heightened antitrust risk.

- *Protection of trade secrets and proprietary business information*. Private sector participants will be reluctant to contribute information containing trade secrets or proprietary business information unless it receives clear protection from general disclosure.

- *Access to government information*. Private sector entities will be reluctant to share other sensitive (though not necessarily proprietary) information with federal government agencies if to do so would make such information subject to public disclosure under laws such as the Freedom of Information Act (FOIA).

- *Protection of sensitive law enforcement and classified national security information*. Governmental entities will be reluctant to contribute information derived from law enforcement and intelligence sources unless it too can be appropriately protected from general public disclosure.

- *National security--International participation*. Parties, including governmental entities, may be reluctant to share sensitive information unless the expected recipients of such information,

particularly foreign nations and multinational corporations, are specified or can be known in advance.

- *State and local participation*. Private sector entities and federal government entities will be reluctant to share sensitive information with state government agencies if to do so would make such information subject to public disclosure under state “sunshine laws.”

Many of these ideas and directions were highlighted for implementation and further study in Presidential Decision Directive 63 (PDD-63). PDD-63 charged the Executive Branch with studying these and other potential "impediments" to information sharing with an eye toward reform. The Department of Justice, with the Office of the National Coordinator and the Critical Infrastructure Coordination Group, has initiated a critical examination of these information-sharing issues, and Mr. Mitchell is prepared to give a status update.

BIOGRAPHICAL SUMMARY

Stevan D. Mitchell is a Trial Attorney with the Computer Crime and Intellectual Property Section of the United States Department of Justice. He has recently completed service as a Member of the President's Commission on Critical Infrastructure Protection (PCCIP) and as part of the Executive Management team for the Critical Infrastructure Assurance Office (CIAO) during its transition to the Department of Commerce. As a PCCIP Commissioner, Mr. Mitchell was responsible for many of the legal studies and recommendations produced and published by the Commission.

As an Trial Attorney with the Computer Crime and Intellectual Property Section, Mr. Mitchell has litigated cases under the Computer Fraud and Abuse Act and provides oversight, consultation and guidance on investigations and prosecutions involving illegal uses of advanced technology. Mr. Mitchell is also the co-author of the Department's intellectual property rights prosecution manual.

Mr. Mitchell has made numerous public appearances, speeches and presentations pertaining to computer crime, electronic search and seizure, criminal intellectual property enforcement, and electronic evidence issues. He has also assumed an active role in the Section's legislative responsibilities, drafting and commenting on legislative proposals with substantial bearing on the investigation and prosecution of high-technology crime.

In the international arena, Mr. Mitchell has participated in several inter-departmental working groups assembled by the Office of the U.S. Trade Representative and the Department of Commerce, and has served as the Department of Justice representative on delegation visits to China, Mexico, Ukraine and Russia. He has also served as host to many international delegations visiting the Department of Justice.

Mr. Mitchell earned his law degree from the Florida State University College of Law, where he served as Editor-in-Chief of the Law Review. After completing a judicial clerkship in the Southern District of Florida, he joined the Criminal Division of the Department of Justice through its Honor Graduate Program.

Nancy J. Wong
Pacific Gas and Electric Company

PRIVATE SECTOR OUTREACH

Both the final report of the President's Commission on Critical Infrastructure Protection (PCCIP) and the Presidential Decision Directive 63 (PDD-63) established private-public partnership as a necessary foundation for protecting the nation's critical infrastructures. It has been estimated that 95% of these infrastructures are owned and operated by private industry and state and local governments. "To succeed, this partnership must be genuine, mutual and cooperative."

Designated federal lead agencies, the National Infrastructure Protection Center, and the National Critical Infrastructure Assurance Office each have a role in the development and implementation of this partnership, as tasked by PDD-63. Foundations of partnering include voluntary participation, mutual goals and benefits, mutual understanding of expectations and objectives, complementary capabilities and roles, frequent interaction, and trust that commitments will be met. Private industry, through its historical experience, tends to be wary of government initiatives. Consequently, a multi-dimensional outreach program that lays out to key audiences an appropriate case for action, as well as a case for partnership, represents the very first step towards engaging industry in a successful partnership.

Ms. Nancy Wong served as a commissioner in 1997 on the President's Commission on Critical Infrastructure Protection as a private industry representative, with experience in both the energy and information technology industries. She took a leave of absence from her position as department head for information assets and risk management with Pacific Gas and Electric Company, where she oversaw the development and implementation of corporate policies, standards and business processes to manage and protect the company's information technology assets. From 1993-1996, Ms. Wong led PG&E's 900-person corporate computer and network operations department. In this position, she managed an annual budget of $60-80 million and the planning and daily operations of the company's entire corporate computing and telecommunications infrastructure, one of the largest private networks in the country. Ms. Wong was selected as one of the "Top One Hundred Women in Computing for 1996" by McGraw-Hill Publishing Companies.

Ms. Wong holds a master's degree in finance and a bachelor's degree in computer sciences and mathematics from the University of California at Berkeley.

Thomas Burke's Position Statement

The General Services Administration was appointed as the Executive Agent for the Federal Sector to oversee the development of an interagency initiative for Presidential Decision Directive 63 (PDD-63). In this initiative, the Federal Sector's Executive Agent assured each department and agency was provided with critical infrastructure protection planning guidance to assist them in the preparation of their Critical Infrastructure Protection Plans (CIPP). As these plans are implemented, departments and agencies are looking to the Federal Sector's Executive Agent for ongoing directional support. This directional support provides a wide range of solution sets through Federal and industry partners focusing on information assurance, vulnerability assessment methodologies, contingency planning techniques and/or research and development planning activities. PDD-63 is an ongoing mandate. Because of this, the Federa1 Sector Executive Agent continues to search for premium methods to assist each department and agency in their ongoing venture to protect the Federal Government's critical infrastructure assets.

Biographical Summary

Mr. Thomas Burke is the Assistant Commissioner for Information Security in the Federal Technology Service of the General Services Administration. Tom has been involved with information systems security for over 32 years. Since joining GSA, Tom has participated in the evolving face of information security and guided the organization in its transition from traditional communications security services to the open systems security services offered today.

Tom is an active participant on the National Security Telecommunications and Information Systems Security Committee (NSTISSC), where he also serves as the Chair of the Subcommittee on Telecommunications Security. He is also the civil agency representative to the Department of Defense Military Communications Electronics Board (MCEB)

Recently, Tom was appointed Chief Infrastructure Assurance Officer (CIAO) for the General Services Administration and the Executive Agent for the Federal Sector in the implementation of PDD-63.

John C. Davis
Director, National Computer Security Center
(410) 854-4371

The Report of the Presidential Commission on Critical Infrastructure Protection was delivered to the White House in October, 1997, and contained 77 recommendations for protecting the critical infrastructures of the United States. As a result, the White House established an Interagency Working Group to determine how the government would respond to this challenging task. The Interagency Working Group released the proposed Presidential Decision Directive (PDD #63). In May 1998, the president signed the PDD and announced the actions to be taken by the entire US government. Mr. Davis will review the Commission's recommendations and highlight how it will affect information professionals within the federal government.

Biographical Summary

Mr. John C. Davis is the Director of the National Computer Security Center at the National Security Agency (NSA) and the NSA representative to the Critical Infrastructure Assurance Office (support for the National Security Council). Mr. Davis served as the NSA Commissioner to the President's Commission on Critical Infrastructure Protection (PCCIP) from April 1997 until October 1998 when the PCCIP office transitioned to the Critical Infrastructure Assurance Office (CIAO). As the lead Commissioner on the Information and Communications team, and the Research and Development team, he was instrumental in developing the Administration's national policy and implementation plan for protecting our nation's most critical infrastructures.

Mr. Davis holds a bachelor's and a master's degree in physics and a master's degree in electrical engineering.