

A presentation featured at the

2010 Topical Symposium:

Economic Security: Neglected Dimension of National Security?

Hosted by:

The Institute for National Strategic Studies

of

The National Defense University

24-25 August 2010

By

GUY COPELAND



Papers presented at NDU Symposia reflect original research by members of NDU as well as other scholars and specialists in national security affairs from this country and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the authors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.

National Infrastructure Protection Plan (NIPP) Partnership Model and Strategic Support for Critical Technology Sectors – DIB and IT

NDU Economic Security Symposium, 24 August 2010



Guy Copeland, Vice President
Information Infrastructure Advisory Programs and
Special Assistant to the CEO, CSC





Defense Industrial Base (DIB) Sector

- The DIB Sector consists of government and private sector organizations that possess capabilities to support military operations directly, perform research and development, design, manufacture, integrate systems, maintain depots, and service military weapon systems, subsystems, components, sub-components, or parts, all of which are intended to satisfy military requirements.



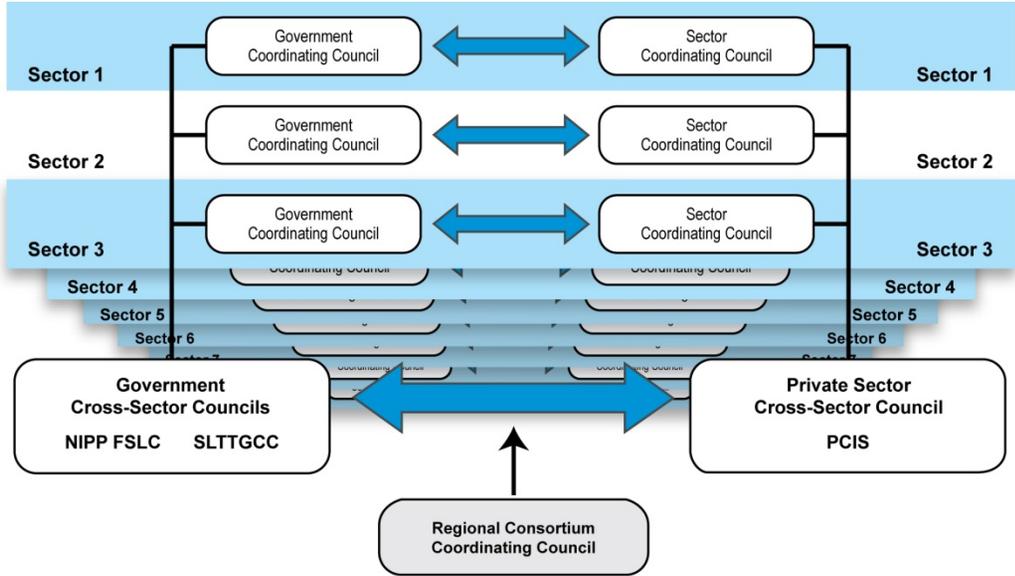
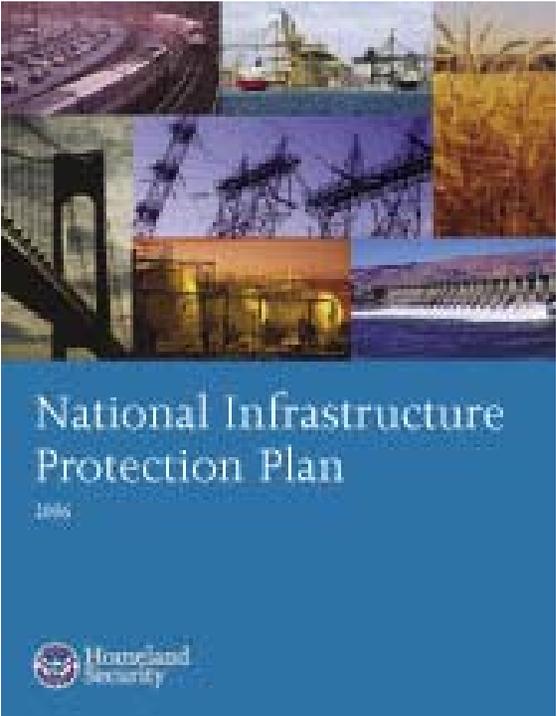
Information Technology (IT) Sector

- Companies and Associations representing:
 - Domain Name System (DNS) root & Generic Top-Level Domain (GTLD) operators
 - Internet service providers (ISPs)
 - Internet backbone providers
 - Internet portal and e-mail providers
 - Networking hardware companies (e.g., fiber-optics makers and line acceleration hardware manufacturers) and other hardware manufacturers (e.g., PC and server manufacturers and information storage)
 - Communications companies that characterize themselves as having an IT role
 - Software companies
 - Security services vendors
 - Edge and core service providers
 - IT system integrators
 - IT security associations



Leveraging DHS Authorities: The National Infrastructure Protection Plan The Critical Infrastructure Partnership Advisory Council

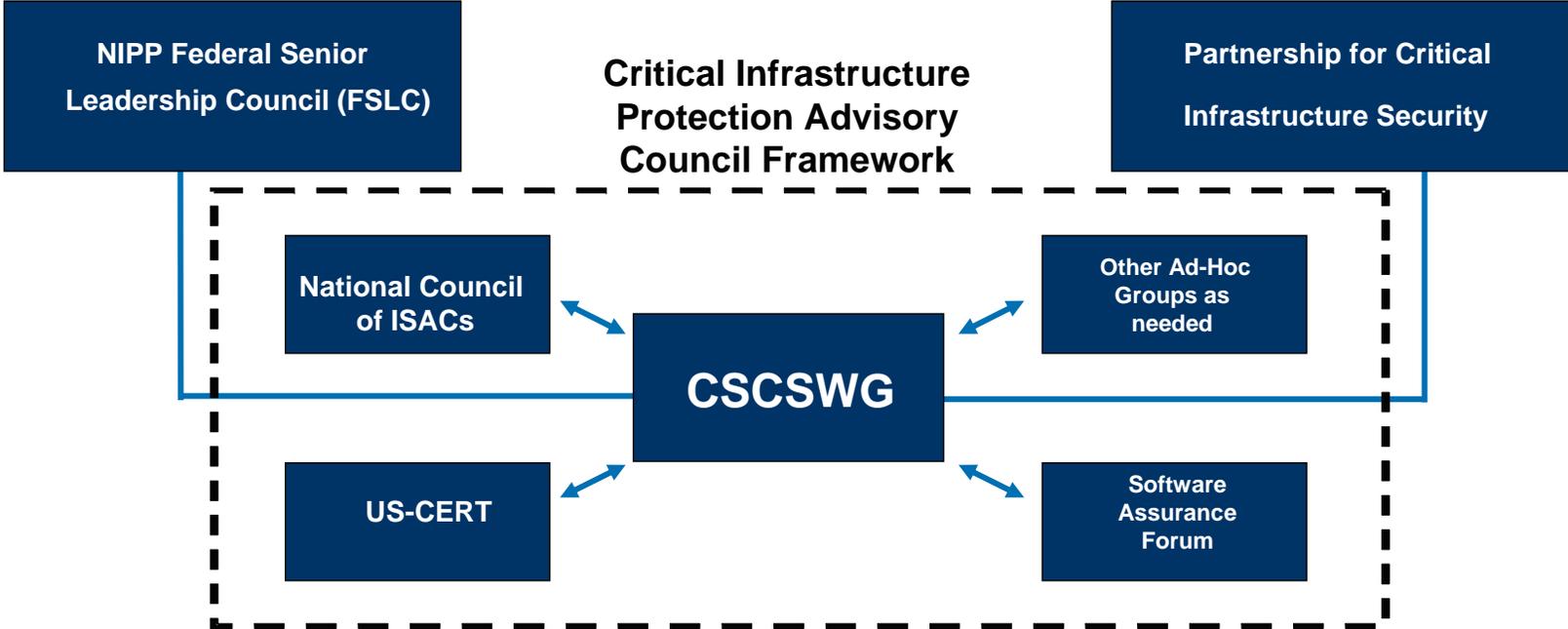
The **NIPP** provides a public-private partnership structure where Federal, state, and local government and private industry owners and operators of critical infrastructure can coordinate on critical infrastructure protection issues.



CIPAC is a regulatory framework created by the Secretary, DHS pursuant to statutory authority granted him by Congress. It permits government and industry within the NIPP structure to have closed meetings, jointly develop programs and initiatives, and coordinate/collaborate on critical infrastructure protection issues outside of the public view but in manners consistent with and accountable to the public interest.



Cross-Sector Cyber Security Working Group CIPAC Framework and Liaison Groups





A Few of Many Strategic Policy Initiatives and Issues

- Partnership status and growth
- International Engagement
- Supply Chain Risk Management
- Enhanced Critical Infrastructure Protection Initiative
- What is “Cyberwar?”
- Human Capital – cyber shortfalls, aging legacy technologists
- Closer operational coordination – especially in cyber
 - DIB Cybersecurity Initiative
 - Enduring Security Framework
 - Mission Assurance Initiative
 - NCIRP and Cyber Storm III
 - National Cybersecurity and Communications Integration Center (NCCIC)
- Regulatory Barriers and Legislative Initiatives