National Infrastructure Protection Plan

Defense Industrial Base Sector

Homeland Security Presidential Directive 7 (HSPD-7) identified 17 critical infrastructure and key resources (CIKR) sectors and designated Federal Government Sector-Specific Agencies (SSAs) for each of the sectors. Under SSA leadership, each sector is responsible for developing and implementing a Sector-Specific Plan and providing sector-level performance feedback to the Department of Homeland Security (DHS), enabling national cross-sector assessments of CIKR protection program gaps. SSAs are responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms for the sector.

Sector Overview

The Defense Production Act of 1950, Executive Order 12919, and Department of Defense (DoD) Directive 5000.60 focus primarily on ensuring adequate industrial capacity in support of national security. In 1998, Presidential Decision Directive 63 identified national defense as a special function in the context of critical infrastructure protection. The July 2002 *National Strategy for Homeland Security,* the February 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* and HSPD-7 identify the Defense Industrial Base (DIB) as a critical infrastructure sector and designate DoD as the SSA.

The DIB Sector includes DoD, government, and the private sector worldwide industrial complex with the capabilities of performing research and development, design, production, delivery, and maintenance of military weapons systems, subsystems, components, or parts to meet military requirements. The DIB Sector includes tens of thousands of companies and their subcontractors who perform under contract to DoD, and companies providing incidental materials and services to DoD, as well as government-owned/contractor-operated and government-owned/government-operated facilities. DIB companies include domestic and foreign entities, with production assets located in many countries. The DIB Sector is dependent upon a number of other sectors, such as Energy, Communications, and Transportation Systems.

The DIB Sector provides products and services that are essential to mobilize, deploy, and sustain military operations. The DIB Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that DoD uses to meet military operational requirements. These requirements, including cyber, are addressed in DoD's broader Defense Critical Infrastructure Program (DCIP), where they are integrated in all DIB Sector activities.

Sector Partnerships

The DIB Sector Coordinating Council (SCC) is a private sector forum of owners and operators who collaborate on protection

measures that may be implemented at their respective facilities. Along with DoD, the Departments of State, Treasury, Justice, Commerce, and Homeland Security have come together to form the DIB Government Coordinating Council (GCC), the government counterpart to the SCC.

These two bodies allow private sector owners and operators to engage with government officials through the Critical Infrastructure Partnership Advisory Council. The Council provides a single venue for internal coordination on a wide range of sector-specific infrastructure protection activities and issues. It further provides a standing forum for government and private sector security partners to: facilitate information sharing; discuss areas of mutual interest; synergistically leverage activities; eliminate duplicative processes; and collaborate on measures necessary to ensure the DIB Sector mission performance.

SCC members, drawn from industry associations, have the authority to represent their respective companies, each of which has significant DIB Sector business interests. Members have broad knowledge of DIB industrial capabilities and security requirements.

CIKR Protection Issues

DIB owners and operators are responsible for protection of DIB Sector assets from hostile threats and hazards. The DoD has limited authority or, in many cases, no authority to perform law enforcement functions or to actively protect the DIB. Critical assets within the DIB are potentially vulnerable to exploitation that could result in DoD mission degradation or failure. The fact that the DIB Sector exists in an open, global environment exacerbates the vulnerability of critical DIB Sector assets.

Furthermore, the changing composition of the DIB Sector (e.g., resulting from mergers and acquisitions as well as shifting wartime priorities) and the evolving regulations and policy that govern the relationship of DoD to the DIB, necessitate broad-based, continuing, long-term interaction among DIB security partners to assure DIB capabilities and reliability. This long-term continuing interaction is vital as the vast majority of critical DIB assets reside in the private sector.

Priority Programs

DoD and the DIB remain cognizant of the threat our Nation faces from current and future hostile elements that could adversely involve our defense industrial facilities. DoD and its DIB partners perform, on an ongoing basis, analyses of products and services provided by defense suppliers that are critical to the Nation's military capability. The "Critical Asset" designation is the result of the coordinated evaluation of: the Offices of the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Chairman of the Joint Chiefs of Staff; the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs; the Defense Contract Management Agency; and the Military Departments and Defense agencies.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.