



National Infrastructure Protection Plan

Defense Industrial Base Sector

Homeland Security Presidential Directive 7 (HSPD-7) identified 17 critical infrastructure and key resources (CI/KR) sectors and designated Federal Government Sector-Specific Agencies (SSAs) for each of the sectors. Each sector is responsible for developing and submitting Sector-Specific Plans and sector-level performance feedback to the Department of Homeland Security (DHS) to enable national cross-sector CI/KR protection program gap assessments. SSAs are responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector.

Sector Overview

The Defense Production Act of 1950, Executive Order 12919, and Department of Defense (DOD) Directive 5000.60 are all focused primarily on ensuring adequate industrial capacity for national security. Presidential Decision Directive 63 identified national defense as a special function of interest in the context of critical infrastructure protection in 1998. 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 assign the responsibility for ensuring DIB functionality to the DOD.

The DIB Sector includes DOD, government, and the private sector worldwide industrial complex with the capabilities of performing research and development, design, production, and maintenance of military weapons systems, subsystems, components, or parts to meet military requirements. The DIB Sector includes more than 100,000 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, some with operations located in many countries. The DIB Sector is dependent upon a number of other sectors, including Energy, Telecommunications, and Transportation Systems.

The DIB Sector provides defense-related products and services that are essential to mobilize, deploy, and sustain military operations. The DIB Sector does not include commercial infrastructure that provides power, communications, transportation, and other utilities that DOD war fighters and support organizations use to meet their operational needs. These activities, including cyber, are addressed in DOD's broader Defense Critical Infrastructure Program (DCIP) and are integrated in all DIB Sector activities.

Sector Partnerships

The DIB Sector Coordinating Council (SCC) is the framework to enable private sector owners and operators to collaborate on protective measures that can be taken for their facilities.

This forum allows private sector owners and operators to engage DOD, DHS, and the SSAs by means of the Critical Infrastructure Protection Advisory Council. The council provides a single point of contact for internal coordination on a wide range of sector-specific infrastructure protection activities and issues. It further provides a recurring forum for DOD and DIB Sector security partners to: facilitate information sharing; identify common areas of interest; synergistically leverage activities; illuminate duplicative processes; and develop a prioritized list, by function area, of required critical infrastructure protection program improvements.

Council membership is comprised of associations representing significant DIB Sector business interests. Members possess an authoritative knowledge of DIB industrial capabilities and security requirements.

The Federal agencies involved in the coordination of the DIB Sector include: DOD; the Departments of Commerce, Treasury, and Justice; and DHS. These Federal agencies have come together to form the DIB Government Coordinating Council (GCC), which is a counterpart to the SCC.

CI/KR Protection Issues

DIB owners and operators protect DIB Sector assets from many potentially hostile threats and hazards. However, the DOD has limited authority or, in many cases, no authority to perform law enforcement functions or to take offensive protective action. 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 susceptibility of critical DIB Sector assets to vulnerability exploitation.

The changing composition of the DIB Sector (e.g., resulting from mergers and acquisitions) and the evolving regulations and policy that govern the relationship of DOD to the DIB necessitates broad-based, continuing, long-term interaction and collaboration with DIB members to ensure DIB capability and reliability. This long-term continuing interaction is vital as the vast majority of critical DIB assets reside in the private sector.

Priority Programs

As we continue to make progress on the Global War on Terrorism, we remain cognizant of the threat our Nation faces from current and future hostile elements that could adversely involve our defense industrial facilities. DOD performs, on an ongoing basis, analyses of various products and services provided by defense suppliers that are deemed critical to this Nation's military capability. The "Critical Supplier" designation is the result of the collective 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; the Defense Contract Management Agency; and the applicable military department and defense agency headquarters.



Homeland
Security

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