

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

Introductory Brief



Homeland
Security

Table of Contents

- Overview
- The Infrastructure Security Landscape
- DHS/NPPD/IP Mission and Authorities
- Core Capabilities
- Organizational Rundown
- DHS/NPPD/IP Strategic Direction



Overview

- The nation's critical infrastructure is what keeps the lights on, the trains running, and the economy moving. It is the foundation of American society, national security, economic stability, and public health and safety
- DHS is the Sector Specific Agency for portions of 10 of the nation's 16 critical infrastructure sectors, and works closely with the SSAs for other sectors
- Infrastructure systems and assets are continued targets and attack surfaces for a wide range of threats and hazards, including both physical and cyber attacks



Overview

- Protecting the nation's critical infrastructure from terrorism and other hazards is core to the DHS national security mission, which faces evolving and increasing threats
- The Office of Infrastructure Protection has been uniquely positioned for this role since DHS was established
 - Unique legal authorities for convening, working with, sharing information and consulting with private sector partners
 - Source of identification of Nation's Critical Infrastructure and associated planning factors
 - Comprehensive national and cross-sector Critical Infrastructure protection and risk management knowledge—including characterizing interdependencies among infrastructure sectors, systems, and assets
 - Field Level, direct support to private sector, state, local, tribal and territorial partners through nationwide staff
 - Outcome-based regulatory program—Chemical Facilities Anti-Terrorism Standards



Critical Infrastructure Impact on the Nation

- 16 critical infrastructure sectors create a widely dispersed network, but sectors are interconnected and interdependent
- Critical infrastructure includes:
 - Vital physical and cyber systems, and networks
 - Thousands of essential energy, water and health facilities, transportation networks, agriculture, defense industry, information technology and other systems



U.S. DEPARTMENT OF
**Homeland
Security**

Critical Infrastructure Faces Evolving Threats



**Homeland
Security**

The National Infrastructure Protection Plan Provides Unity of Effort to the Mission



**Owners &
Operators**



**State, local, tribal,
territorial, regional
governments**



**Non-governmental
organizations**

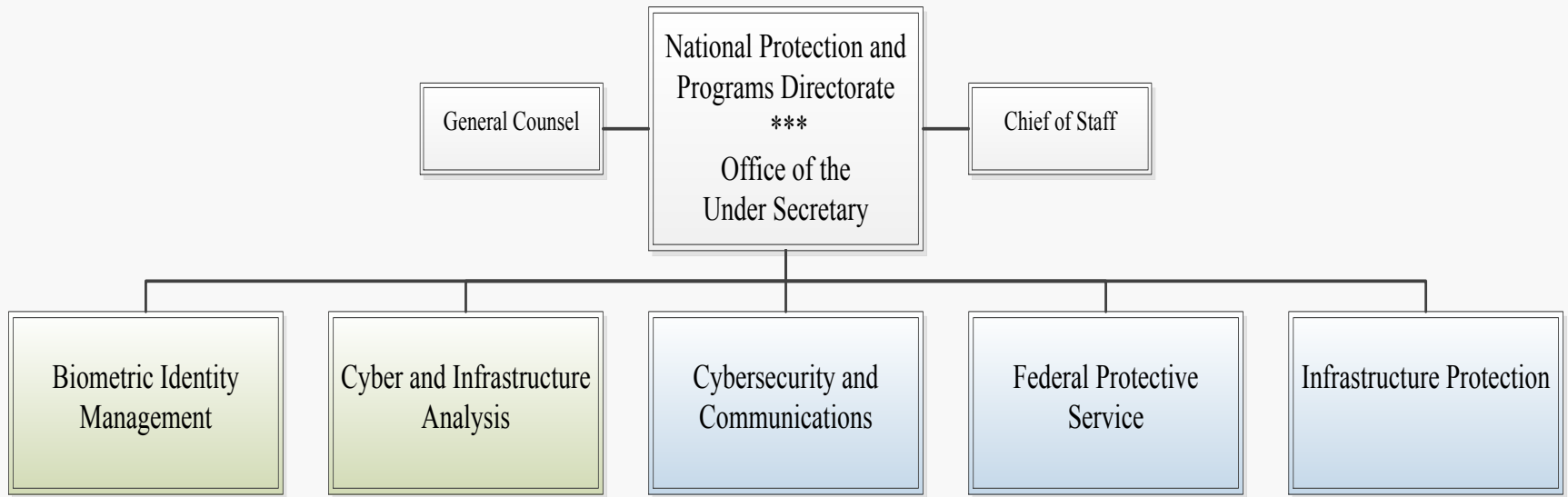


**Federal
Government**

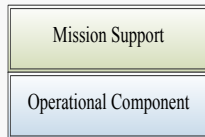


**Homeland
Security**

NPPD Organizational Overview

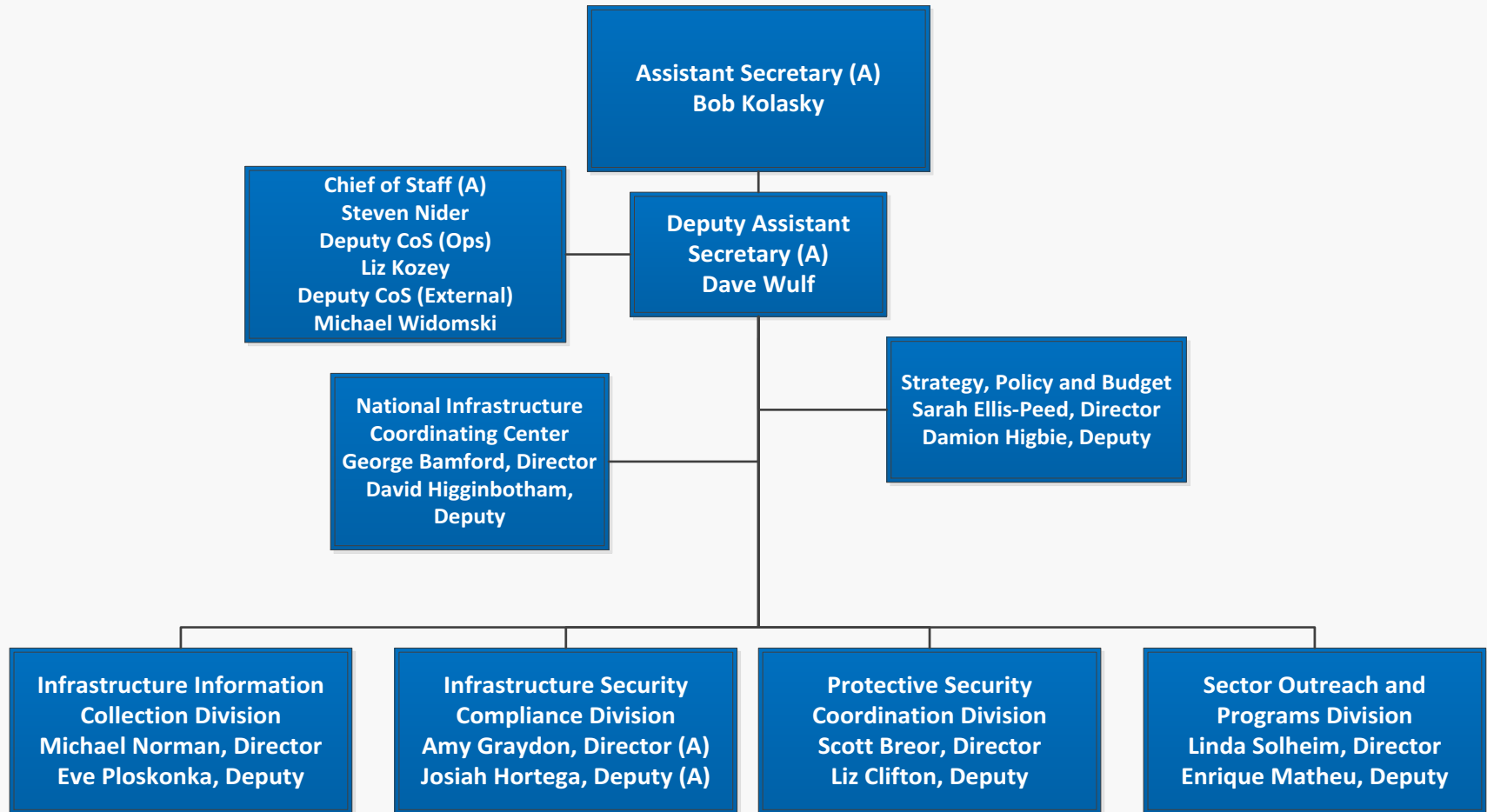


Key:

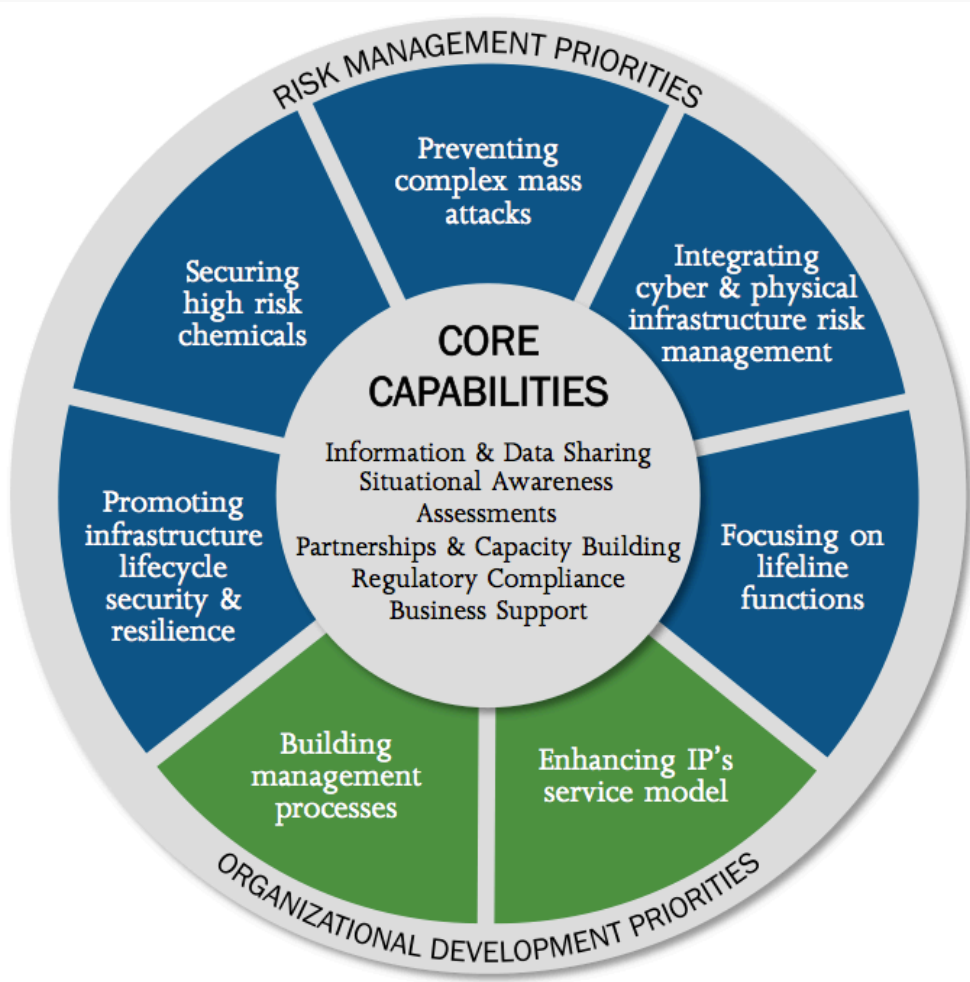


**Homeland
Security**

IP Organizational Overview



IP's Core Capabilities Address Specific Priorities through Specialized Programs and Offices



Homeland Security Counter-Improvised Explosive Device & Risk Mitigation Training

To reduce risk to the Nation's critical infrastructure, the Department of Homeland Security's Office for Bombing Prevention (OBP) develops and delivers a diverse

Homeland Security Multi-Jurisdiction Improvised Explosive Device Security Planning

The Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDGP) Program is a systematic process that fuses counter-IED capability analysis, training, and planning to enhance urban area IED prevention, protection, mitigation, and response capabilities. The MJIEDGP assists with collectively identifying roles, responsibilities, capability gaps and with

Homeland Security Penalties for Violations of the Protected Critical Infrastructure Information (PCII) Program

The Protected Critical Infrastructure Information (PCII) Program, part of the Department of Homeland

Homeland Security Protective Security Advisor Program

The Office of Infrastructure Protection (IP) operates the Protective Security Advisor (PSA) Program. PSAs facilitate field activities in coordination with IP divisions and other Department of Homeland Security (DHS) offices. The PSA Program maintains a robust operational field capability, conducting assessments of nationally significant critical infrastructure through Enhanced Critical Infrastructure Protection (ECIP) security surveys, Site Assistance Visits, and incident response and providing access to IP resources, training, and information.

PSA Program

Established in 2004, the PSA Program's primary mission is to protect critical infrastructure. The five mission areas mentioned below are carried out in direct support of this primary mission objective. Regional directors (RDs) and PSAs also conduct crosscutting information sharing and coordination activities in support of these mission areas:



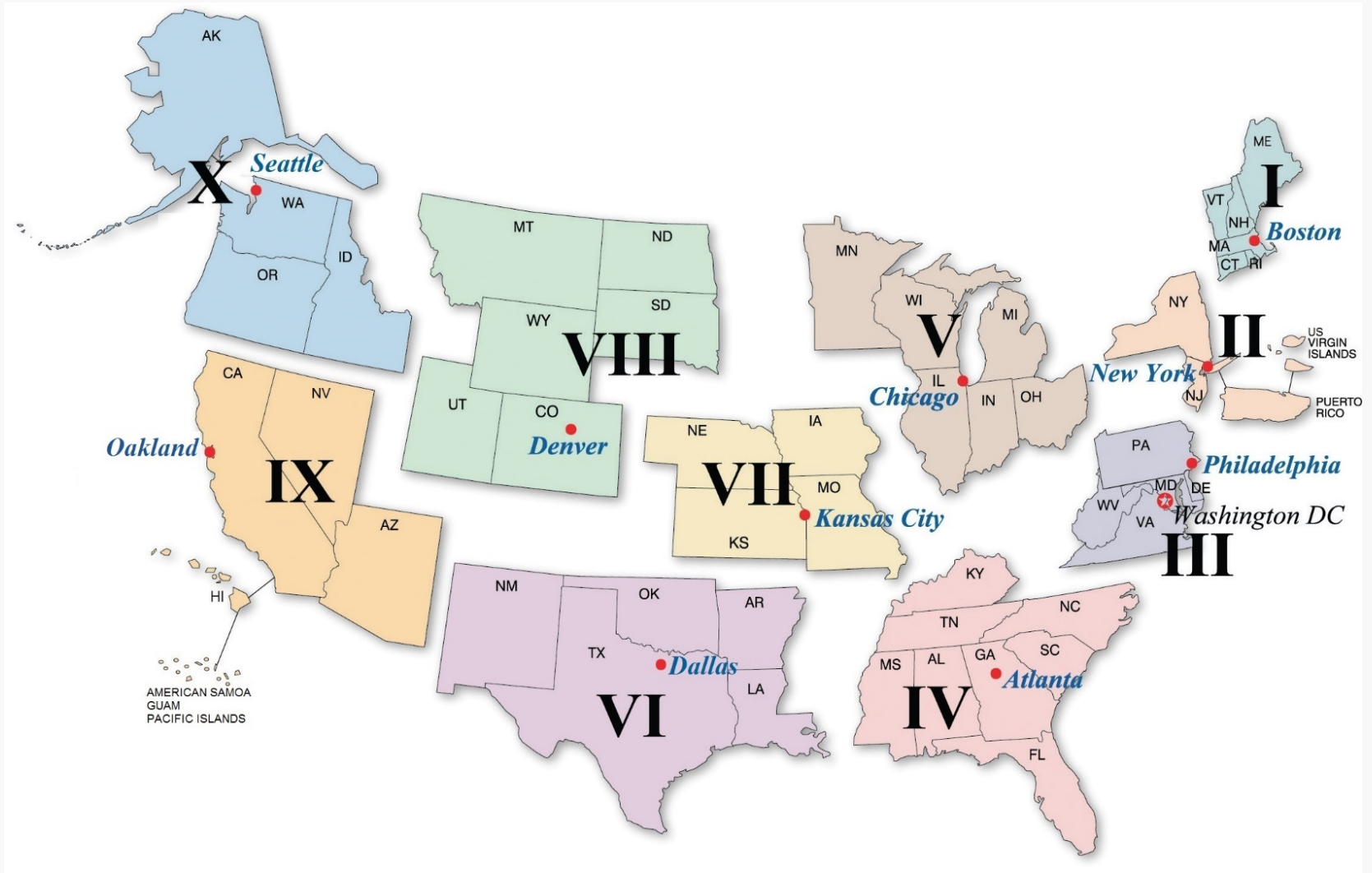
Homeland Security

Key IP Programs and Activities

- Critical Infrastructure Partnership Advisory Council (CIPAC)
- Protective Security Advisors (PSAs)
- Regional Resiliency Assessment Program (RRAP)
- Active Shooter Preparedness
- Vulnerability Assessments
- National Infrastructure Coordinating Center (NICC)
- Exercises
- SSA for 6 Sectors
- Private Sector Clearance Program (PSCP)
- Protected Critical Infrastructure Information (PCII) Program
- IP Gateway
- Chemical Facility Anti-Terrorism Standards (CFATS)
- Ammonium Nitrate Security Program
- Interagency Security Committee (ISC)
- Office for Bombing Prevention (OBP)
- Position Navigation and Timing (PNT) Program Management Office
- National Infrastructure Advisory Council



Regional Office Locations/Coverage





Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure
