



Defense Critical Infrastructure Program Overview and Assessment Summary



Mr. Todd Spangler
Defense Critical Infrastructure Office
Office of the Assistant Secretary of Defense
Homeland Defense & Americas' Security Affairs

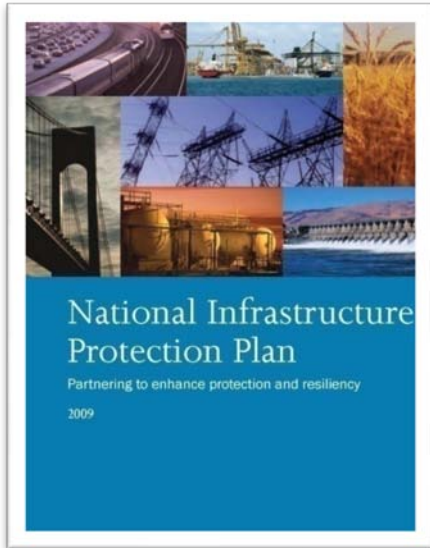
Presentation to:

Governor's Hurricane Conference
May 26, 2010



POLICY

National and Departmental Authorities

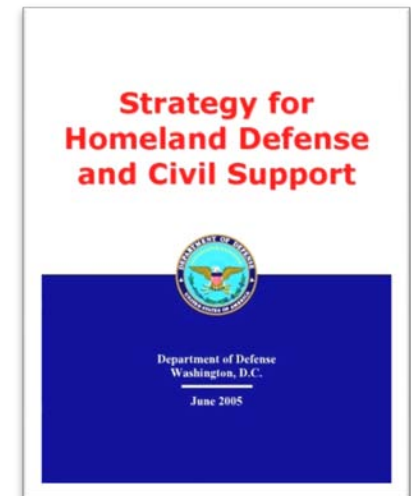


HSPD 7 – National framework for critical infrastructure protection

- ❑ **Broad national role and a focused DoD role for the DCIP**
 - 18 Critical Infrastructure and Key Resource sectors; DoD is Sector-Specific Agency (SSA) for Defense Industrial Base sector
 - All federal departments and agencies will *“identify, prioritize, assess, remediate, and protect their respective internal critical infrastructure and key resources.”*
- ❑ **Implementation guidance in the *National Infrastructure Protection Plan (NIPP)***

Strategy for Homeland Defense and Civil Support – Departmental guidance for HSPD-7 implementation

- ❑ Key Objective: *“...achieve mission assurance through...ensuring the security of defense critical infrastructure.”*
- ❑ Requires implementation of policy and programs to ensure:
 - Preparedness and protection of defense critical infrastructure
 - Preparedness of the national Defense Industrial Base (DIB)





POLICY

Defense Critical Infrastructure Program

What is DCIP?

- ☐ A DoD risk management program that seeks to ensure the availability of assets deemed critical to DoD missions.

- ☐ Includes DoD and non-DoD domestic and foreign assets essential to planning, mobilizing, deploying, executing, and sustaining U.S. military operations on a global basis.

- ☐ DCIP risk management involves taking actions to prevent, correct, or minimize risks associated with vulnerabilities.



Defense Critical Infrastructure Program

What does DCIP do?

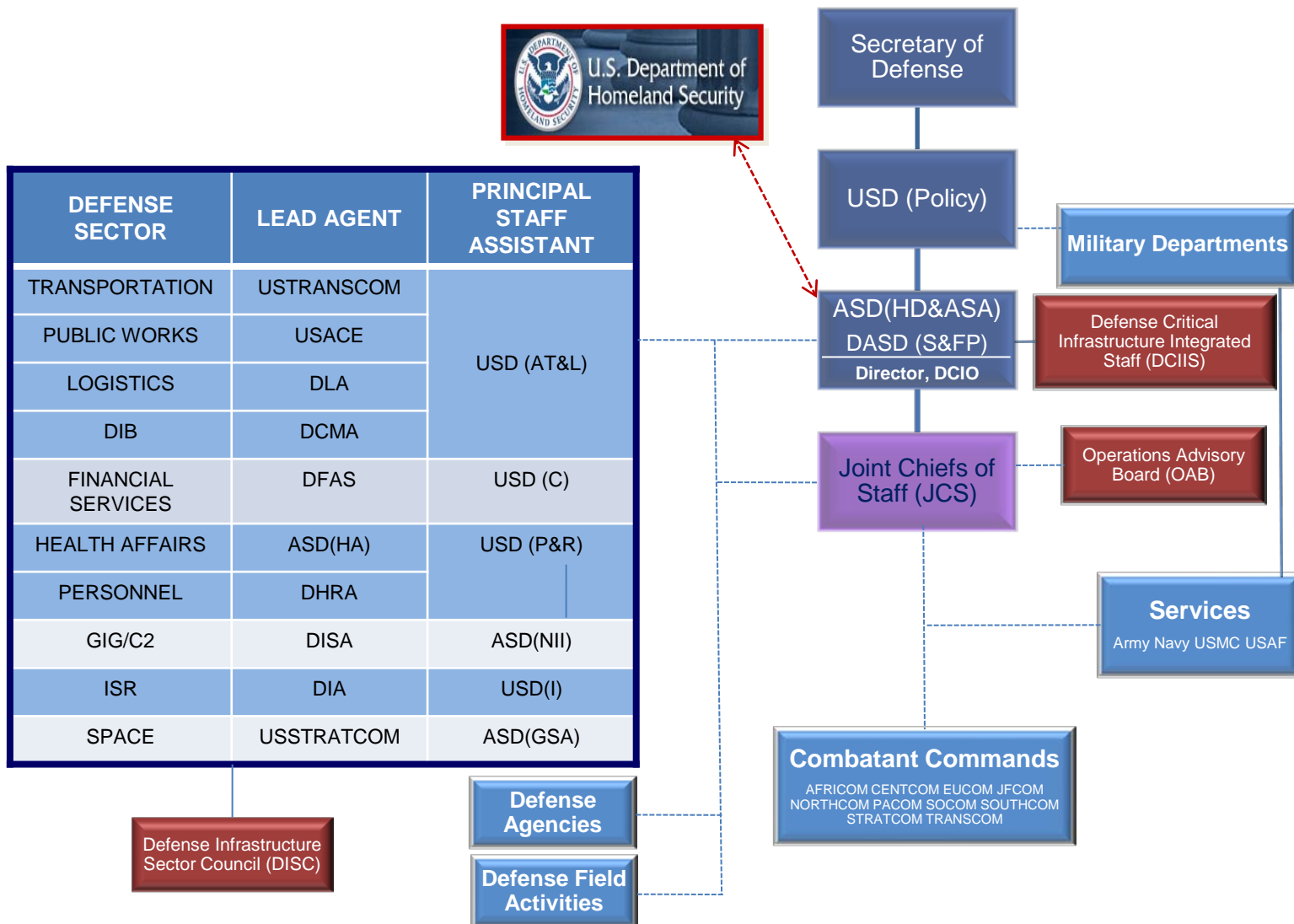
- ❑ **DCIP enables management of risk through risk assessment which:**
 - Establishes the criticality of assets
 - Assesses the vulnerabilities of assets
 - Identifies threats and hazards

- ❑ **Decision makers then use the results of the assessment to determine appropriate risk response measures:**
 - Accept the risk
 - Minimize the impact of a potential threat or hazard (i.e. mitigation)
 - Correct or eliminate identified vulnerabilities (i.e. remediation)
 - Restore lost capability in the aftermath of an event (i.e. reconstitution)



POLICY

DCIP Stakeholders





Geospatial Data Fusion

❑ HSIP Gold and Freedom

- Foundational data for majority of viewers and information systems

❑ DCIP Stakeholder Data

- COCOMS, Services, Sectors
- Assets identified through the Critical Asset Identification Process (CAIP)

❑ Other Infrastructure Databases

- DoD compiles and maintains numerous data sets
- Other government data (federal state/local)
- Proprietary data from commercial sector (utilities, associations)





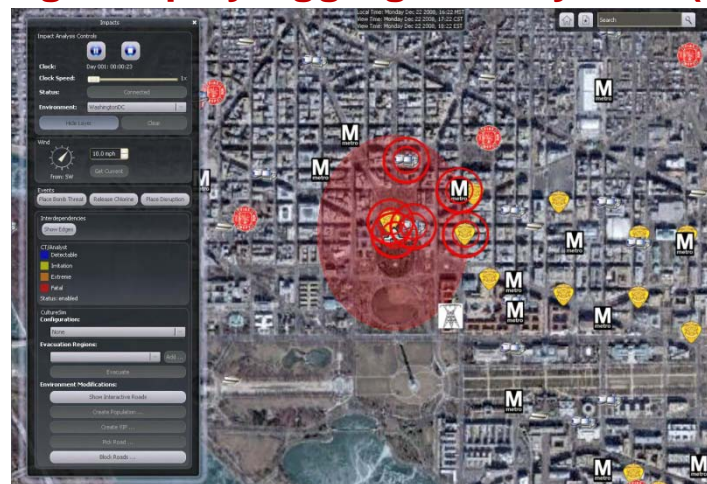
POLICY

Common Operational Pictures

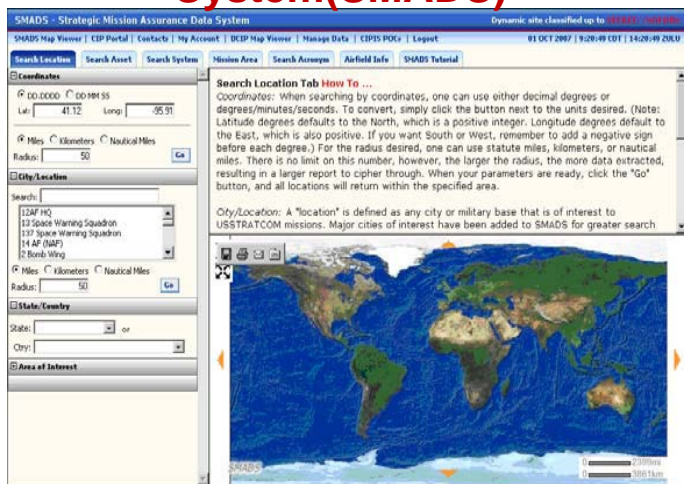
TRITON



Knowledge Display Aggregation System (KDAS)



Strategic Mission Assurance Data System (SMADS)



Homeland Defense Mission Assurance Portal (HD-MAP)





POLICY

Contact Information



Todd Spangler

Defense Critical Infrastructure Office
Office of the Assistant Secretary of Defense for Homeland
Defense and Americas' Security Affairs
703.699.5727
todd.spangler@osd.mil