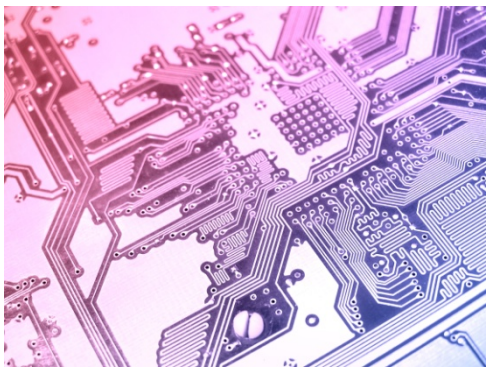
2008 DIB Critical Infrastructure Protection Conference & Technology Exhibition

Mr. Pete Verga
Principal Deputy ASD (HD&ASA)

POLICY

Agenda

- The Challenges We Face
- The National Security Environment
- DoD Preparedness & Response
  - Physical
  - Cyber
- Conference Challenge



POLICY

Welcome

The DIB is a worldwide industrial complex with capabilities to develop and maintain military weapons systems to meet military requirements

- +250,000 Defense Industrial Base (DIB) Sites worldwide
- DIB is critical to our nation and the war fighter
- DIB assets support DoD missions
- Vital to the DoD execution of the National Military Strategy
- Our collective efforts make a difference in war fighter's lives and missions

DoD values your contributions to maintain technologically superior, resilient industrial capabilities to preserve our nation's security.

POLICY

National Security Environment-Security Assessment

Nation-state threats will continue

- ❑ "Traditional" ballistic and cruise missile threats
- ❑ Rogue states employing asymmetric means
  - ➢ Both cyber and physical
- ❑ Potential emergence of a regional peer competitor

Natural Hazards

- ❑ Earthquake
- ❑ Flood, Tsunami
- ❑ Wildfire
- ❑ Health and Disease

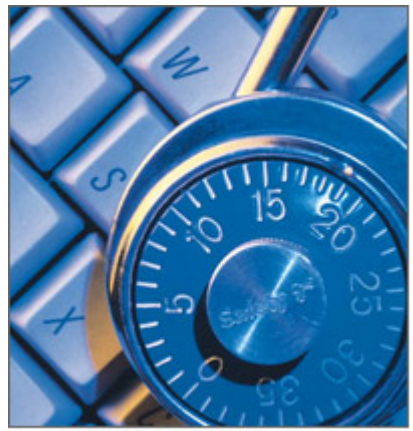
Transnational threats will be the most pressing

- ❑ Terrorists will seek to:
  - ➢ Attack Americans and Western Allies at home and abroad
  - ➢ Inflict mass casualties or cause mass panic through CBRN means (e.g., CBRN weapons or conversion of civilian infrastructure or transport into WMD)

POLICY

Challenges

- Collaboration
  - Partnership, shared responsibility, and Trust engendered by partnership
  - Information sharing and protection
  - Threat and warning information sharing
- HUMINT (Insider threat)
- Physical Threats and Hazards
- ***Cyber Security***



"Each of us has an extremely important role to play in protecting the infrastructures and assets that are the basis for our daily lives and that represent important components of our national power and prestige. The success of our protective efforts requires close cooperation between government and the private sector at all levels. "

- President George W. Bush

POLICY

Mission Assurance Concept

- Improve DoD's ability to execute its Mission Essential Functions in a stressed environment through integrating key programs & activities
- Comprehensively evaluate risk to DoD missions, including the unintended consequences of base consolidation & realignment
- Enable Senior Leader's ability to refine mission-related policies, plans, programs, resources, and activities, and more productively link policy decisions to operational requirements through:
  - Organizational Effectiveness
  - Funding Efficiencies – Making better informed resource allocation (e.g. budgetary) decisions that increase oversight and accountability
  - Compliance – Coordinating and consolidating Measures of Effectiveness (MOEs)

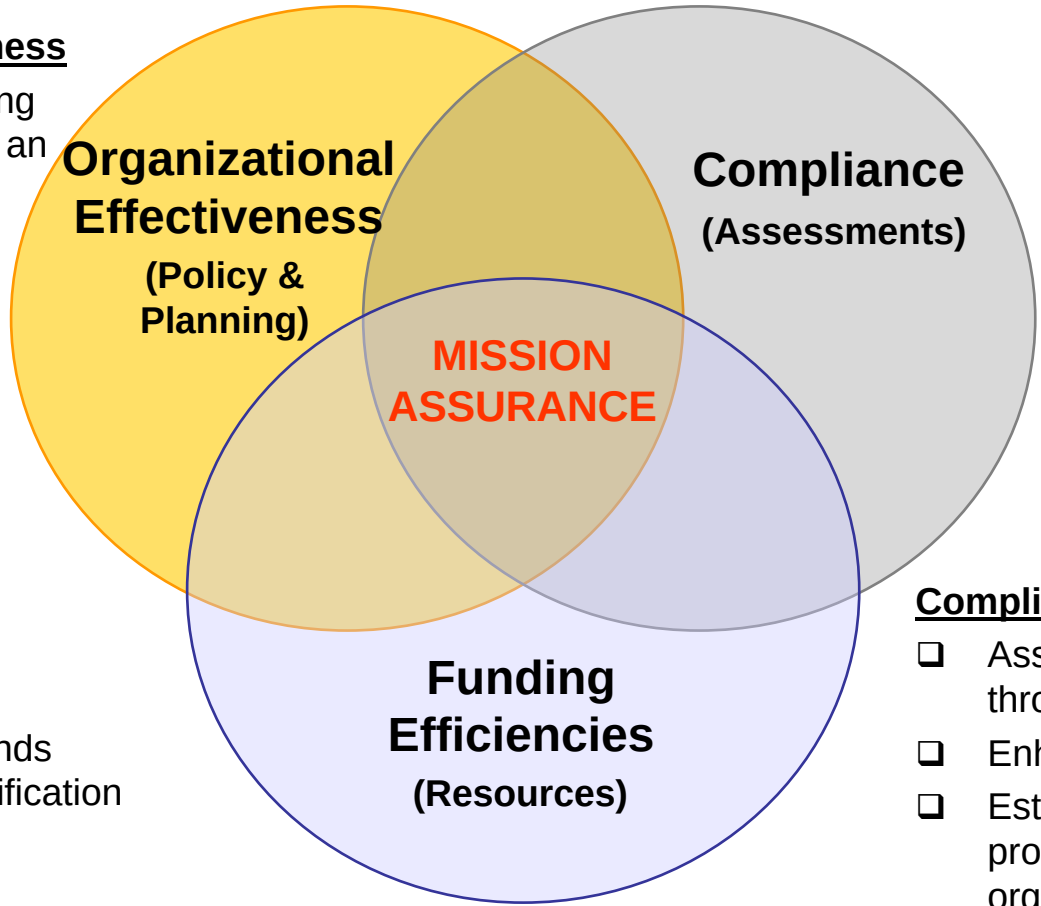
Mission Assurance is an integrating concept, NOT a change of ownership!

POLICY

Mission Assurance – A Value Proposition

Organizational Effectiveness

- ❑ Improves relations among segregated elements of an organization
- ❑ Integrates disparate elements
- ❑ Improves operational efficiency and mission effectiveness



Funding Efficiencies

- ❑ Improves cost control
- ❑ Improves access to funds through prioritized justification of needs
- ❑ Prioritizes funding and resource allocation

Compliance

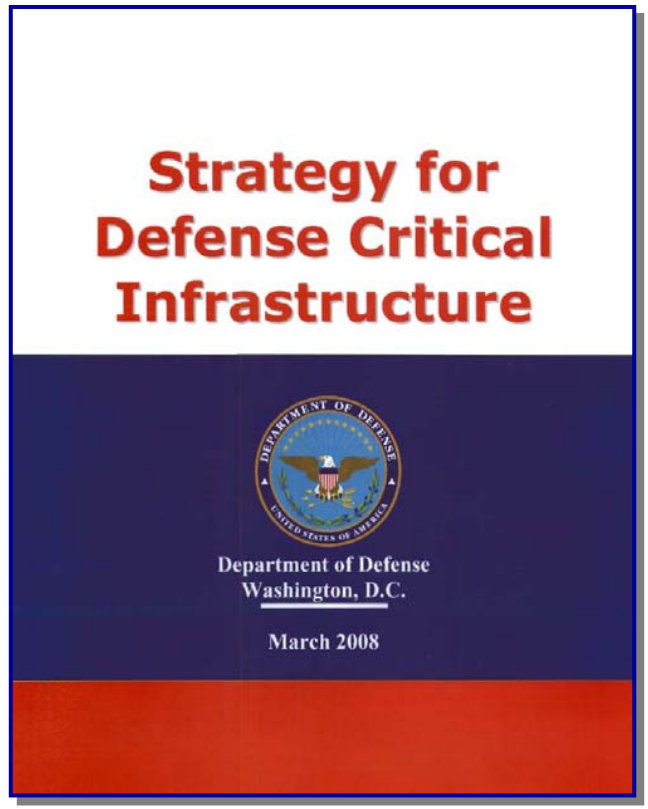
- ❑ Assures commitment throughout organization
- ❑ Enhances readiness
- ❑ Establishes governance process internal to the organization
- ❑ Accounts for applicable legislative requirements

Strategy for Defense Critical Infrastructure

POLICY

- Articulates DoD's risk management approach required for ensuring the availability of assets deemed essential to the successful completion of DoD missions in an all-threat, all-hazard environment

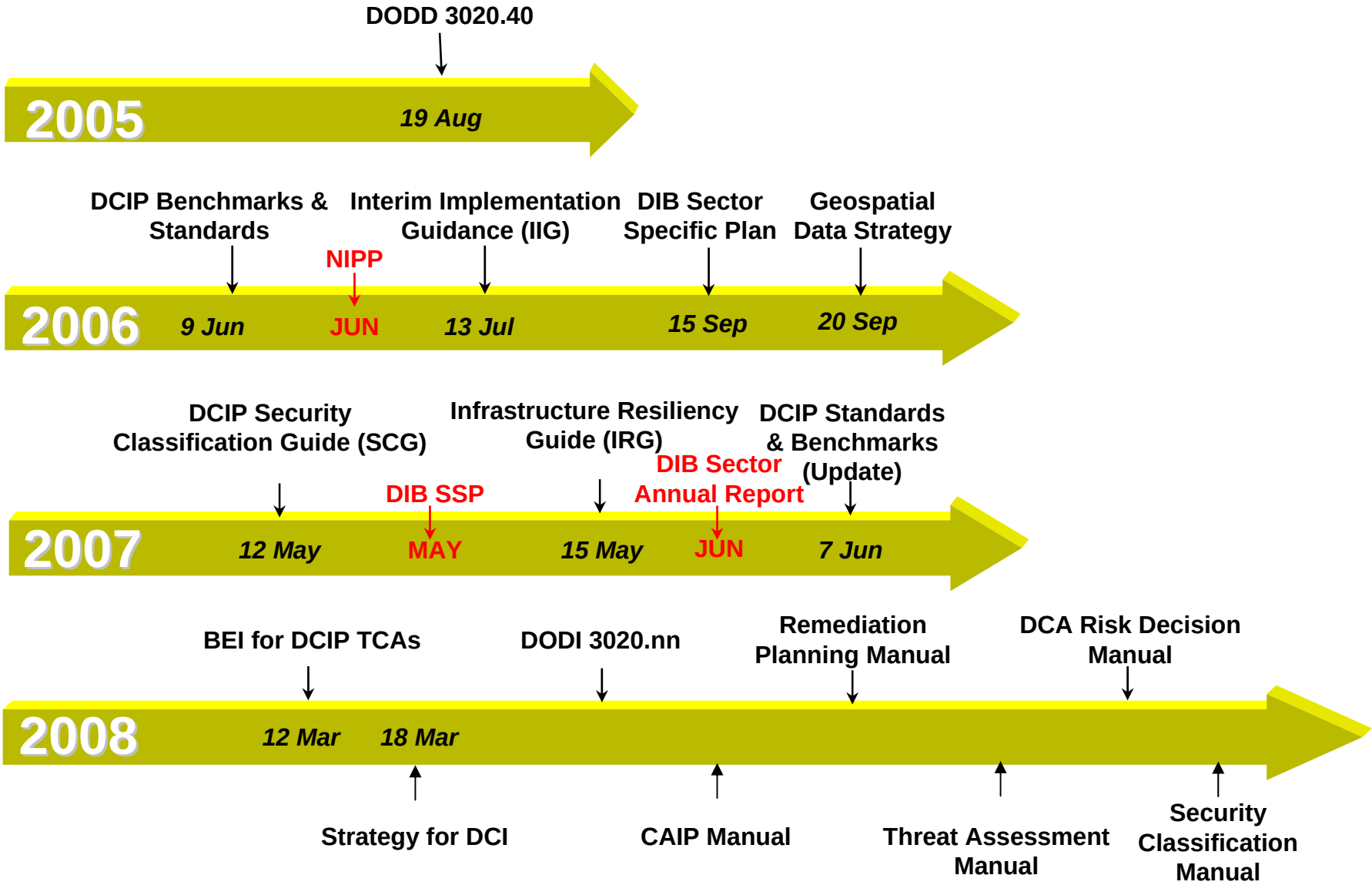
- Defines through stated goals & objectives how DoD will protect Defense Critical Infrastructure (DCI) to achieve mission assurance



  - **Goal 1: Provide DCIP policy and program guidance**
  - **Goal 2: Foster DCIP strategic partnerships and enabling technologies**
  - Goal 3: Integrate and implement DCIP plans, programs, and capabilities at all levels
  - Goal 4: Facilitate DCIP resourcing at all levels
  - Goal 5: Promote DCIP education and outreach

DCIP Strategic Policy Timeline

POLICY



POLICY

Partnering

- Partnering Leads to Real Success
  - Rotating electrical equipment / control system vulnerability
  - CIP-MAA assessment visits – information for owner/operator use
  - BZPP provided resources to improve first responder capabilities
  - Providing security awareness training for DIB partners
- Government and Private Sector
  - Team effort to produce the Sector Specific Plan – continues to grow
    - CIPAC public / private working group on Goals and Objectives
    - CIPAC public / private working group on cyber security
  - DCMA and DHS Protection Security Advisor visits
- Canadian Dept of National Defence (DND)
  - Establishing mutual awareness and assessment program (e.g. Joint Strike Fighter)

POLICY

Partnering Efforts

- DoD-DIB Information sharing
  - Providing best practices, expertise and information
- DoD-DIB collaboration on response actions
  - Response actions
  - Self-assessments
- Protected Critical Infrastructure Information (PCII)
  - Protects voluntarily submitted critical infrastructure information (CII) from public release under FOIA, civil litigation, and state and local "sunshine" laws.
  - ASD (HD&ASA) continues to pursue DoD accreditation under this program.

Leverage trust for two-way communication and share information for a shared purpose – assured availability

POLICY

Cyber Threat

- Hostile nations still pose a cyber threat to the United States because they have the intent and technological capabilities to do so.

- A cyber attack could substantially impact a number of sectors in the United States, including agriculture, emergency response and preparedness systems, transportation, energy, health care, financial services, and telecommunications.

Cyber Attacks are a REAL and EMERGING National Security Threat


AC360
CNN

POLICY

Cyber Security

- Cyber Security is a **National Effort**
  - DHS is lead agency for domestic cyber security
  - DoD will fully support national efforts with policy coordination, information sharing, and technology transfer
- DepSecDef directed USD(P) to lead **Cyber Security Task Force**
  - Chartered to implement NSPD-54/HSPD-23, Cyber security Policy
  - DoD members include NII, SOLIC, ATL, J5, Air Staff, and JTF-GNO
  - Interagency partners include DHS, DOJ, OTSP, DNI, and NSA
- ASD HD&ASA has DoD DCIP **mission oversight and policy responsibility**
  - Lead cyber security coordinator for DoD
  - Best positioned to interface with the interagency and leverage existing capabilities and competencies within DoD

Provide unity of effort across the Department and coordinate with interagency partners to improve national security against the full spectrum of cyber threats

POLICY

Conference Challenge

- What do you perceive as the greatest threats to CI/KR IT and communications networks?
- What are gaps and barriers to effective bi-directional information sharing?
- What types of information sharing are existing public-private partnerships and structures best at addressing?
- How can we share best practices, products, and standards?
- What existing and emerging technologies do you believe are most essential to enhanced CI/KR network security?

2008 DIB Critical Infrastructure Protection Conference & Technology Exhibition

QUESTIONS?

WE'RE AT WAR

ARE YOU DOING ALL YOU CAN?