Homeland Security

S&T Stakeholders Conference

Risk-Informed Requirements Process

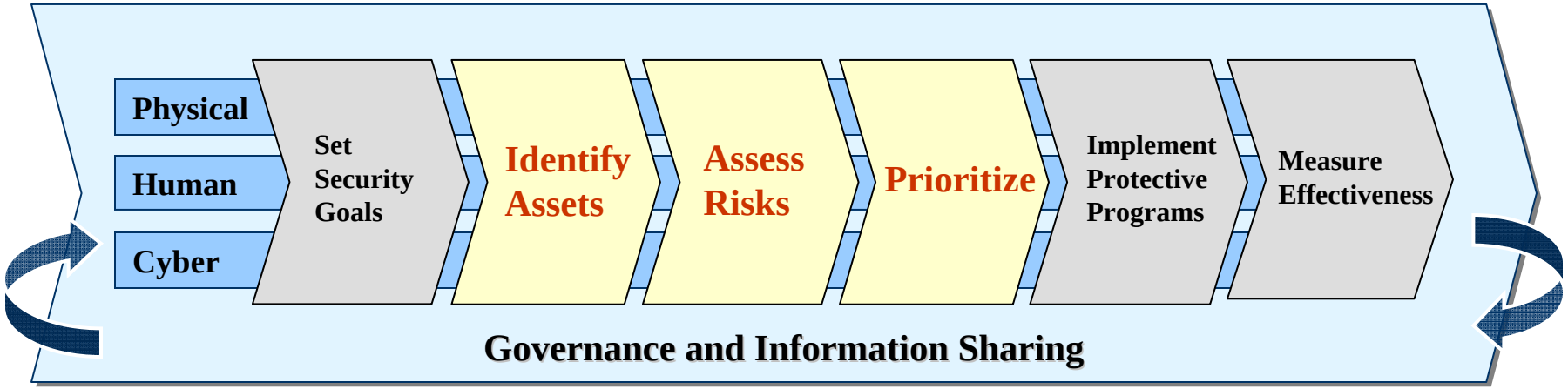
Col. Merrick Krause, USAF (Ret.)
Director
Infrastructure Analysis & Strategy Division
U.S. Department of Homeland Security

June 2-5, 2008

PARTNERING FOR A SAFER NATION

National Infrastructure Protection Plan (NIPP)

- Operational framework for protecting the **17 Critical Infrastructure/Key Resources (CI/KR) sectors**
- Provides a clear **division of labor** between infrastructure protection and our Federal, State, local, tribal, and private sector partners
- Forms the basis for **risk-based** CI/KR protection requirements and prioritization
- Informs the annual Federal **budget process** in infrastructure protection mission area

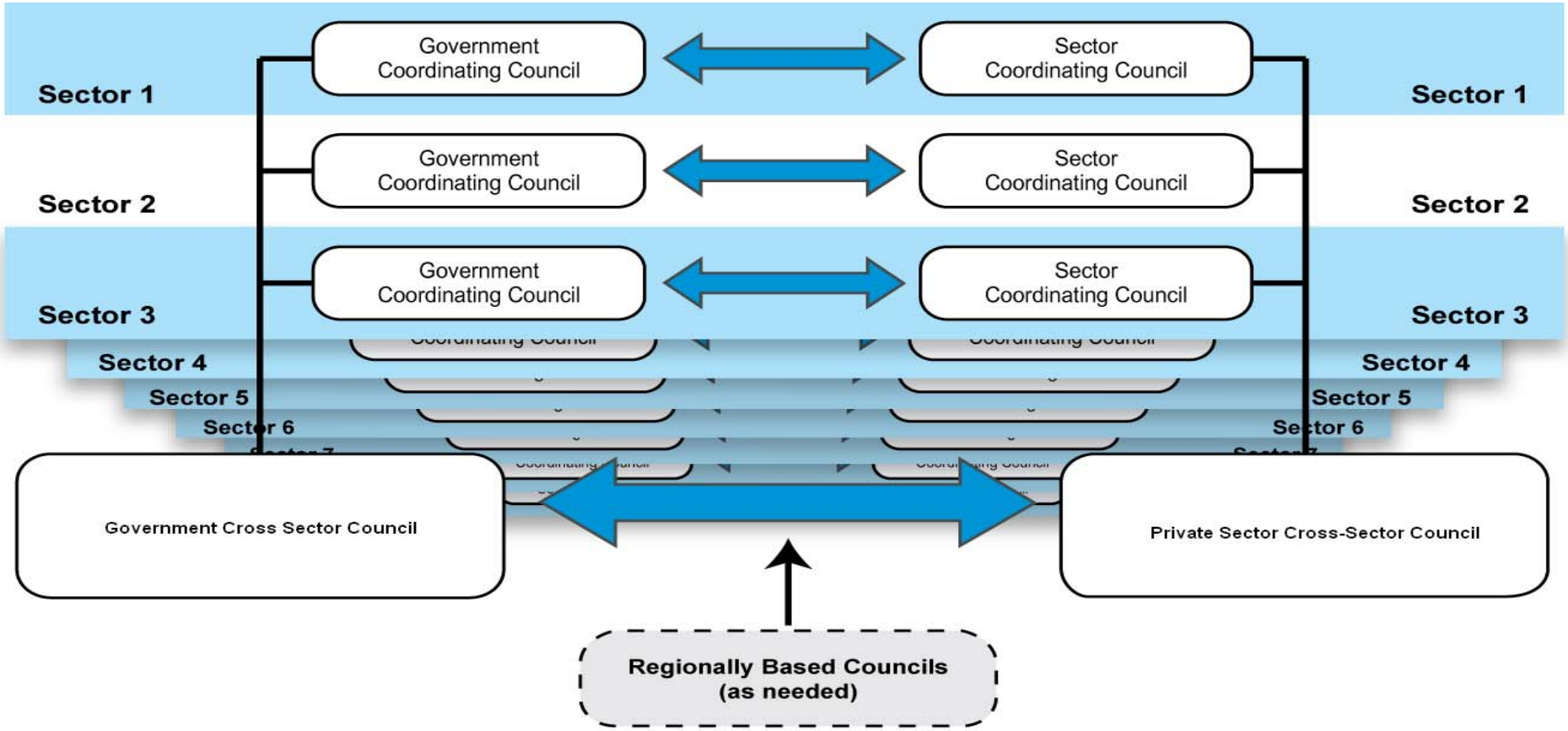


The NIPP risk management framework uses **threat, consequence, and vulnerability information** to produce comprehensive and systematic **assessments** that drive CI/KR risk reduction

Homeland Security

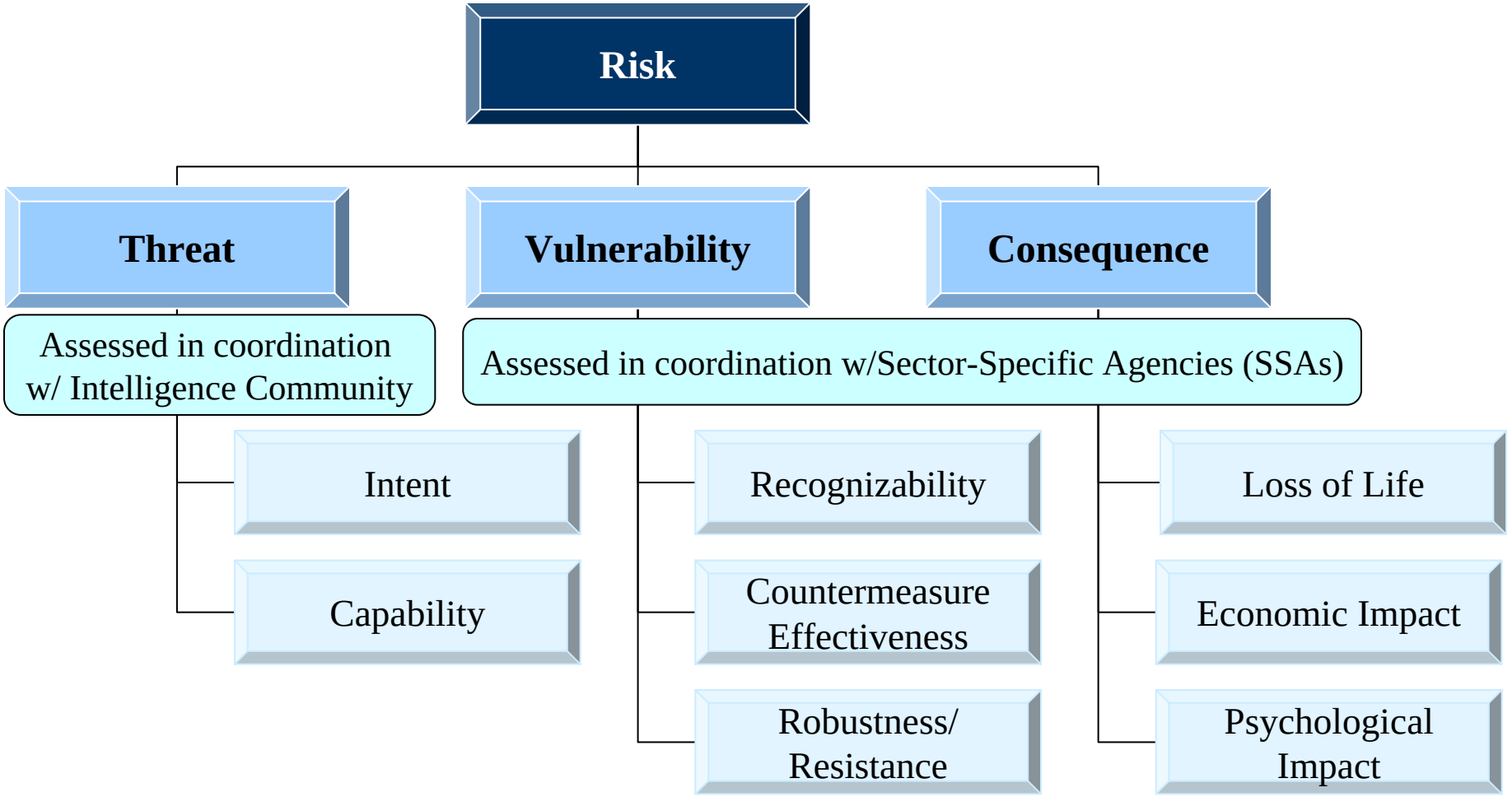
NIPP Partnership Model

- Creates a forum for the requirements collection process
- Involves 2-way collaborations with private sector, Federal agencies, States, Territories, local governments, and tribal security partners



Homeland Security

Assessed Components of Risk



Homeland Security

Risk Analysis Components

Infrastructure Analysis & Strategy Division (IASD)

- Homeland Infrastructure Threat & Risk Analysis Center (HITRAC)
  - Joint Program Office between IP and I&A conducting threat and risk analysis
  - Risk analysis for all sectors
  - Influences approximately $2-3B in DHS grants
- National Infrastructure Simulation and Analysis Center (NISAC)
  - Congressionally mandate center for critical infrastructure protection
  - Operations support with all-hazards modeling, simulation, and analysis
  - Capabilities with and between all sectors (consequence analysis, cascading effects, interdependencies)
- R&D Analysis Branch
  - Focal point for emerging technology and risk reduction
  - Leads joint CIKR Sector R&D requirements process
  - Enhanced interaction with S&T Directorate and full spectrum of potential collaborators (Centers of Excellence, university programs, etc.)

Homeland Security

Strategic Homeland Infrastructure Risk Assessment (SHIRA)

- Provides a snapshot of the risks to the Nation's CIKR, including physical and cyber assets from international terrorists and their affiliates:
  - Determines the highest risks to the nation from attacks targeting the CI/KR sectors
  - Addresses risk based on existing threat, vulnerability and consequence data, but does not speculate on how these variables will evolve
- Basis for the National CIKR Risk Profile within the National CIKR Protection Annual Report
- HITRAC coordinates directly with the stakeholders to obtain or generate the data used in the assessment:
  - Work with the Intelligence Community to assess threat
  - Work with the SSAs and other Federal subject matter experts to assess vulnerability and consequence by CIKR sector

Tier 1/Tier 2 Program

- Through collaborative process with Federal partners, and State and territorial government partners, DHS has identified ~3,000 Tier 1/Tier 2 assets and systems based upon objective consequence and criticality-based criteria
- Designed to increase accuracy of prioritization efforts that inform DHS resource allocation decisions, focus planning, and support effective incident management, response and restoration activities
- The Tier 1/Tier 2 results will be used to:
  - Provide common basis for which DHS & partners to implement CI/KR protection initiatives
  - Support eligibility determinations for largest Homeland Security Grant Programs
  - Ensure assets/systems capable of creating significant consequences are primary focus of DHS protective efforts

Homeland Security

Natural Disaster Preparedness

- The National Infrastructure Simulation and Analysis Center (NISAC) produced 10 detailed hurricane impact studies covering the East Coast from Texas to Maine
  - Broadly distributed them within DHS and to external partners to support pre-event planning
  - Studies provide comprehensive hurricane impact analysis on CIKR in affected area, highlighting critical assets (Tier 1/Tier 2 and others), as well as assets that have significant cascading effects
- DHS provides specific impact studies for all hurricanes Category 2 and above that are scheduled to make landfall
- Provide updated analysis and respond to specific analytical requests year round (e.g., prioritize facilities for restoration, protection, DHS leadership-requested preplanned analyses, etc.)

Homeland Security

Risk-Based Requirements Process

- Collected and re-organized Sector Annual Report (SAR) capability gaps/requirements chapter
  - SAR utilizing new “capability gaps template” for tracking and management
  - R&D Tiger Teams consulted with sectors to help articulate requirements
  - IP staff has emphasized Sector-Specific Agencies for contact thus far
  - Integrated S&T Critical Infrastructure Protection (CIP) R&D Plan with SAR and CIKR Annual Report
- Created and used Requirements Steering Group (cross-functional team of IP and S&T division directors) to evaluate and prioritize requirements/capability gaps
  - Used matrix analysis to identify CIKR sector R&D requirements that were completely unaddressed in S&T IPT process
- Presented gaps and SMEs to S&T Transition for use in Dec 07 Integrated Product Team (IPT) Capstones and other S&T research centers/vendors
  - Used SHIRA & other criteria for risk-informed prioritization

Homeland Security

Conclusion

- Risk is cornerstone in identifying and prioritizing grants, disaster preparedness activities, CIKR Sector requirements, and potential R&D projects
- Threat, vulnerability, and consequences are key components in calculating risk
- All risk-related projects and analyses for the Office of Infrastructure Protection fall within National Infrastructure Protection Plan (NIPP) framework

Bottom Line:

- DHS' customer-driven R&D process **needs** deliberate, authoritative risk-informed decisions to allow prioritization of limited resources

Homeland Security

Homeland Security