

George Mason University's Security Analysis & Risk Management Association

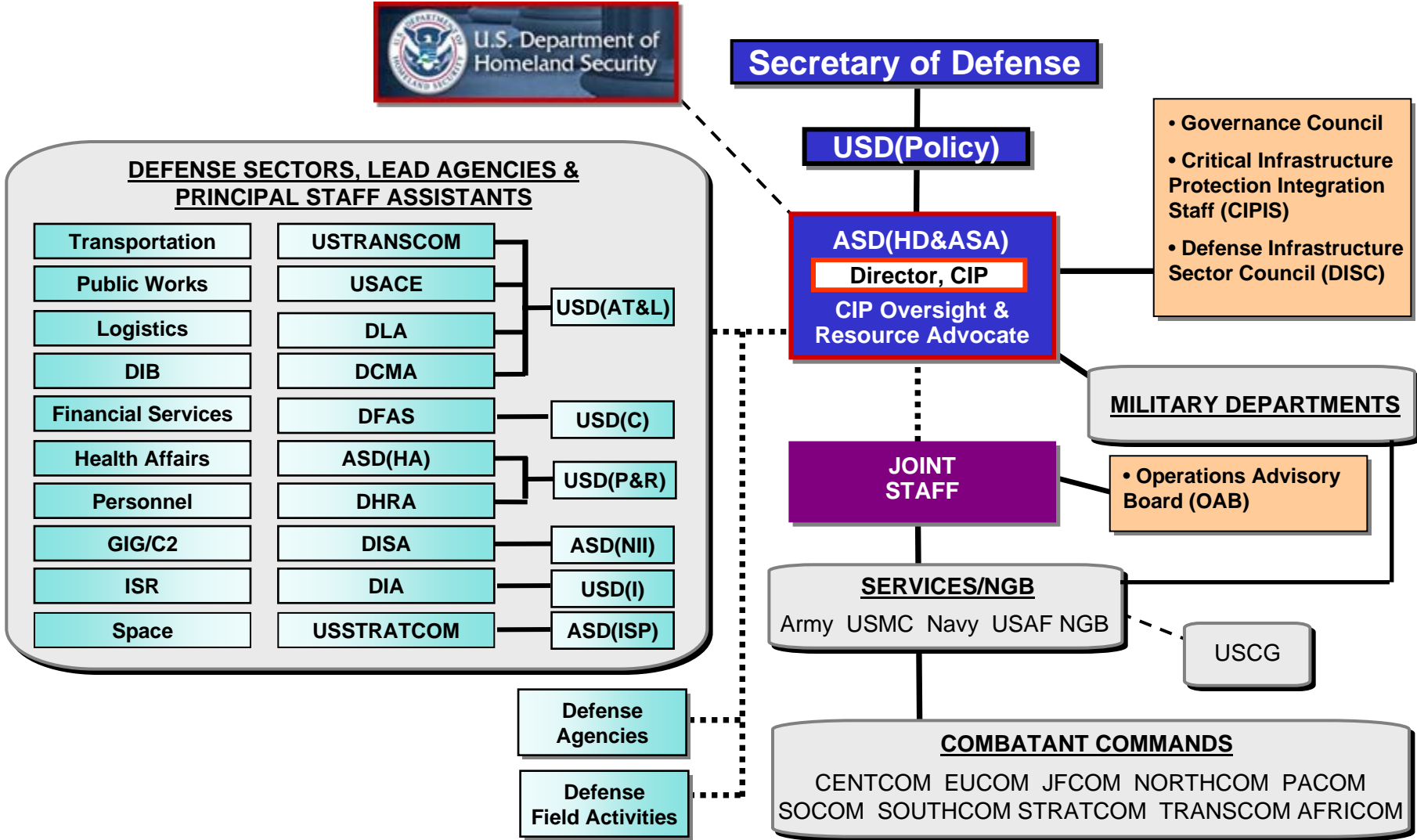


**Mr. Derek 'Dirk' Maurer
Deputy ASD (CM&MA)**



POLICY

DoD CIP Organizational Framework

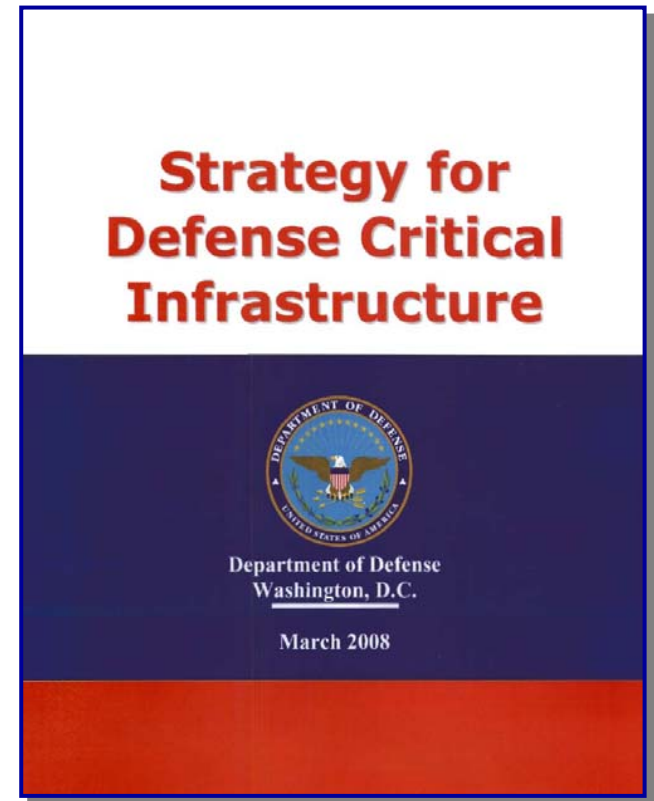




Strategy for Defense Critical Infrastructure

POLICY

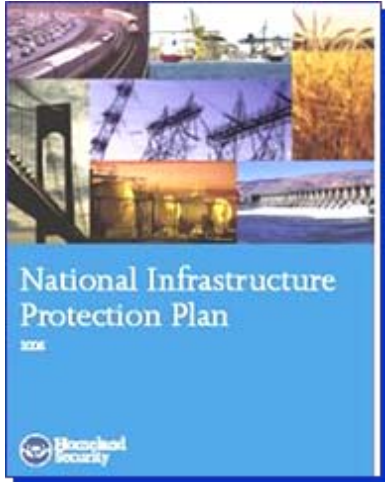
- ❑ Articulates DoD's risk management approach required for ensuring the availability of assets deemed essential to the successful completion of DoD missions in an all-threat, all-hazard environment
- ❑ Defines through stated goals & objectives how DoD will protect Defense Critical Infrastructure (DCI) 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





National and Department Policy

POLICY

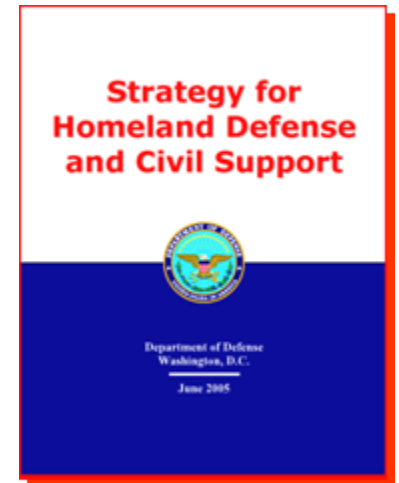


HSPD 7 – National framework for critical infrastructure protection

- ❑ Broad national role and a focused DoD role for the DCIP
 - 17 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

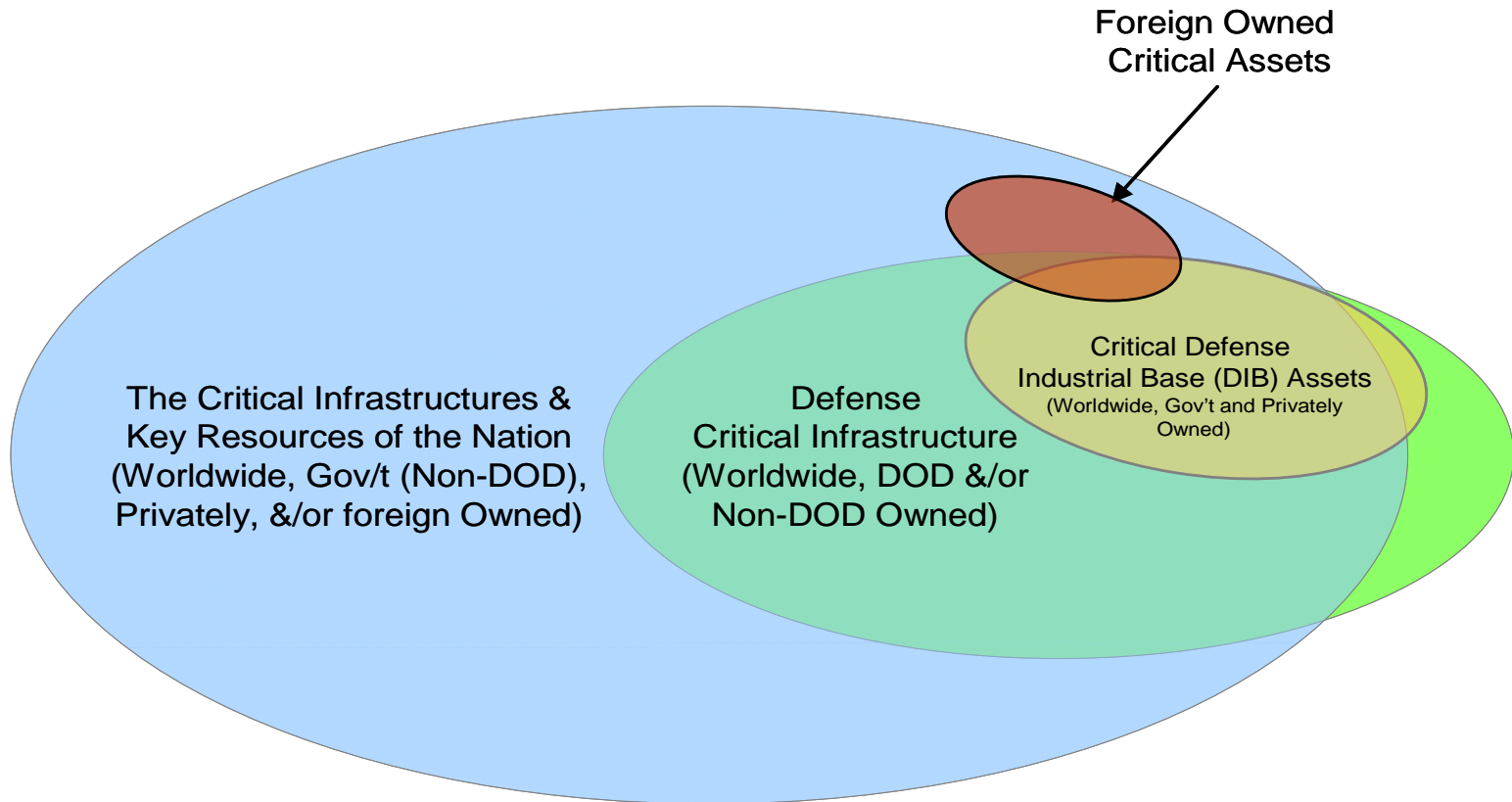
- ❑ Key Objective: *“...achieve mission assurance through...ensuring the security of defense critical infrastructure.”*
- ❑ Requires implementation of policy and programs to ensure:
 - Preparedness and protection of defense critical infrastructure
 - Preparedness of the national Defense Industrial Base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





POLICY

Critical Infrastructure Protection Framework



National Critical Infrastructure and associated key resources provide the capability for the nation to respond to threats to the U.S. homeland. DOD further identifies Defense Critical Infrastructure essential to DOD's execution of the National Defense Strategy. The Defense Industrial Base is vital to this capability. Some of these critical assets may be foreign (e.g. government or privately) owned.



Defense Critical Infrastructure Program *Homeland Security Presidential Directive (HSDP)-7*

POLICY

- Enhance the protection of our Nation's critical infrastructure and key resources against terrorist attacks
- Identify, prioritize and coordinate the protection of critical infrastructure and key resources in order to prevent, deter and mitigate the effects of deliberate efforts to destroy, incapacitate or exploit them.
- **Work closely with State and local governments and the private sector.**

NATIONAL CI/KR SECTORS

Department of Agriculture

- Agriculture, food (meat, poultry, egg products)

Department of Health and Human Services

- Public Health and healthcare
- Food (other than meat, poultry, egg products)

Environmental Protection Agency

- Drinking water and wastewater treatment systems

Department of Energy

- Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)

Department of the Treasury

- Banking and Finance

Department of the Interior

- National monuments and icons

Department of Defense

- **Defense Industrial Base**

Department of Homeland Security

- Security
- Chemical
- Commercial facilities
- Dams
- Emergency services
- Commercial nuclear reactors, materials, and waste
- Information Technology
- Telecommunications
- Postal and shipping
- Transportation systems
- Government facilities



POLICY

Defense Critical Infrastructure Program *Sector-Specific Agency Responsibilities*

- Collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
- Conduct or facilitate vulnerability assessments of the sector; and
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources



DCIP Risk Management Process

POLICY

- It is neither practical nor feasible to protect all of our infrastructure, assets or resources. Therefore we must take steps to ensure the availability of that which is deemed most critical to our missions.

- DoD will protect DCI through a risk management approach that supports the prioritization of scarce resources, while focusing priorities on assets at greatest risk, based on assessed *criticality*, *vulnerability*, and *threats & hazards*

- Risk Assessment
 - Identify Critical Assets
 - Identify Threats & Hazards
 - Identify Vulnerabilities

- Risk Decision

- Risk Response
 - Accept Risk
 - Mitigate the Threat/Hazard
 - Remediate the Risk
 - Reconstitute Lost Capability



POLICY

Simple Risk Model and the DCIP Approach

C. Search for vulnerabilities (4 + 5)

Don't waste DCIP energy or \$\$\$ finding and fixing these

or these

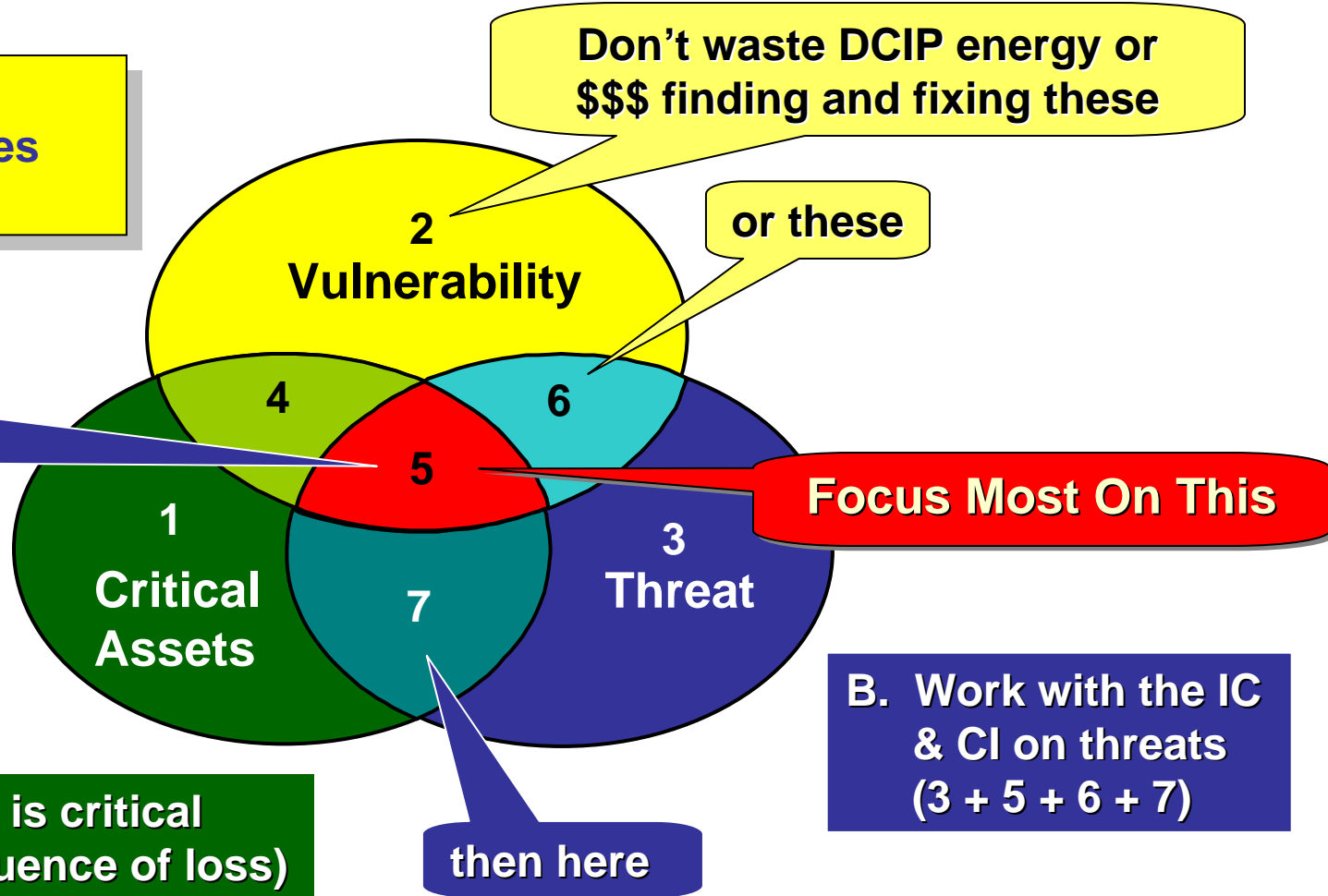
Assess Threats & Hazards here

Focus Most On This

A. Identify what is critical (high consequence of loss) (1 + 4 + 5 + 7)

B. Work with the IC & CI on threats (3 + 5 + 6 + 7)

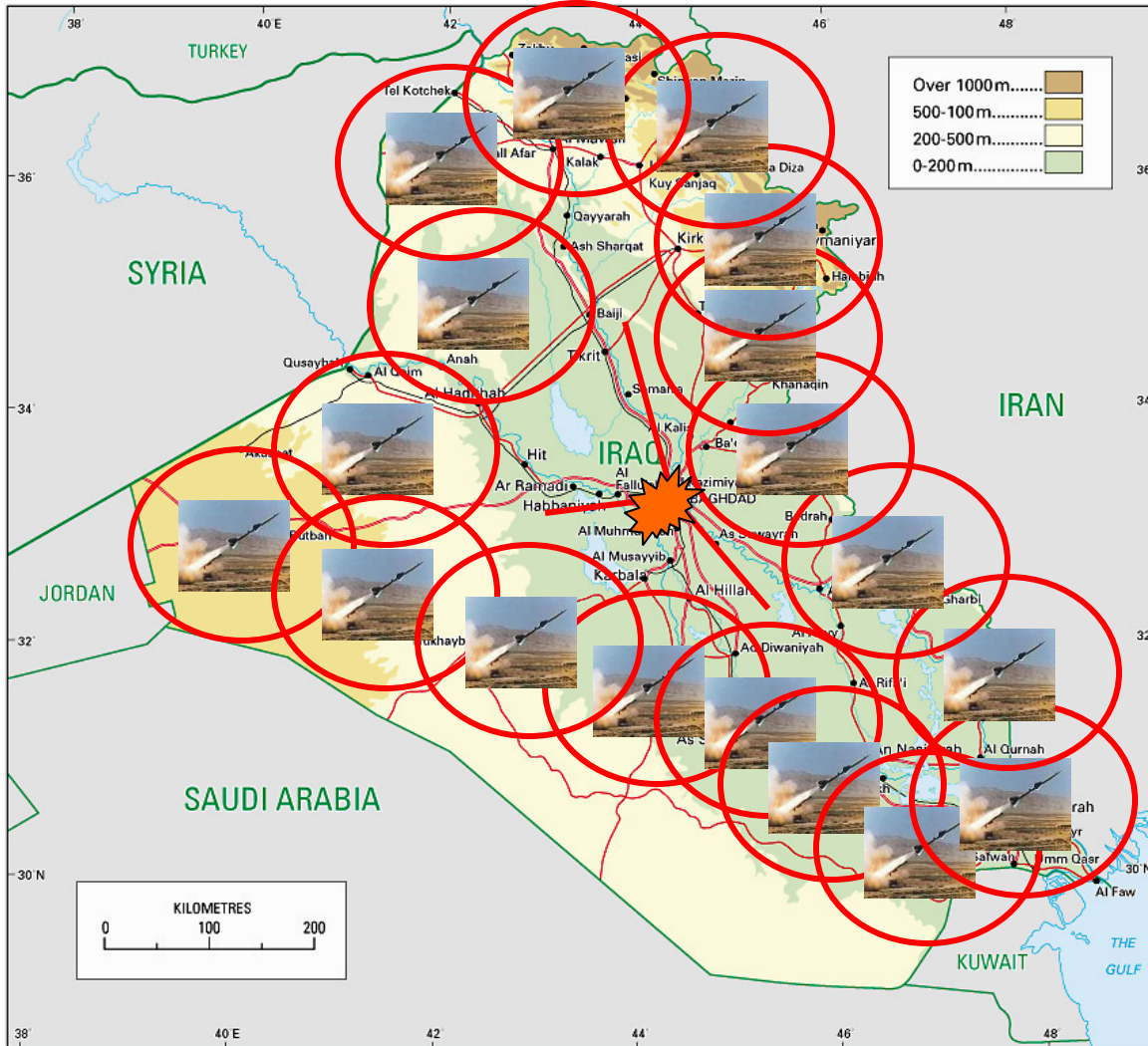
then here





POLICY

DCIP Example



On 16 Jan 1991, Iraq had an air defense system 7 times more lethal than what the U.S. faced over Hanoi in 1970.

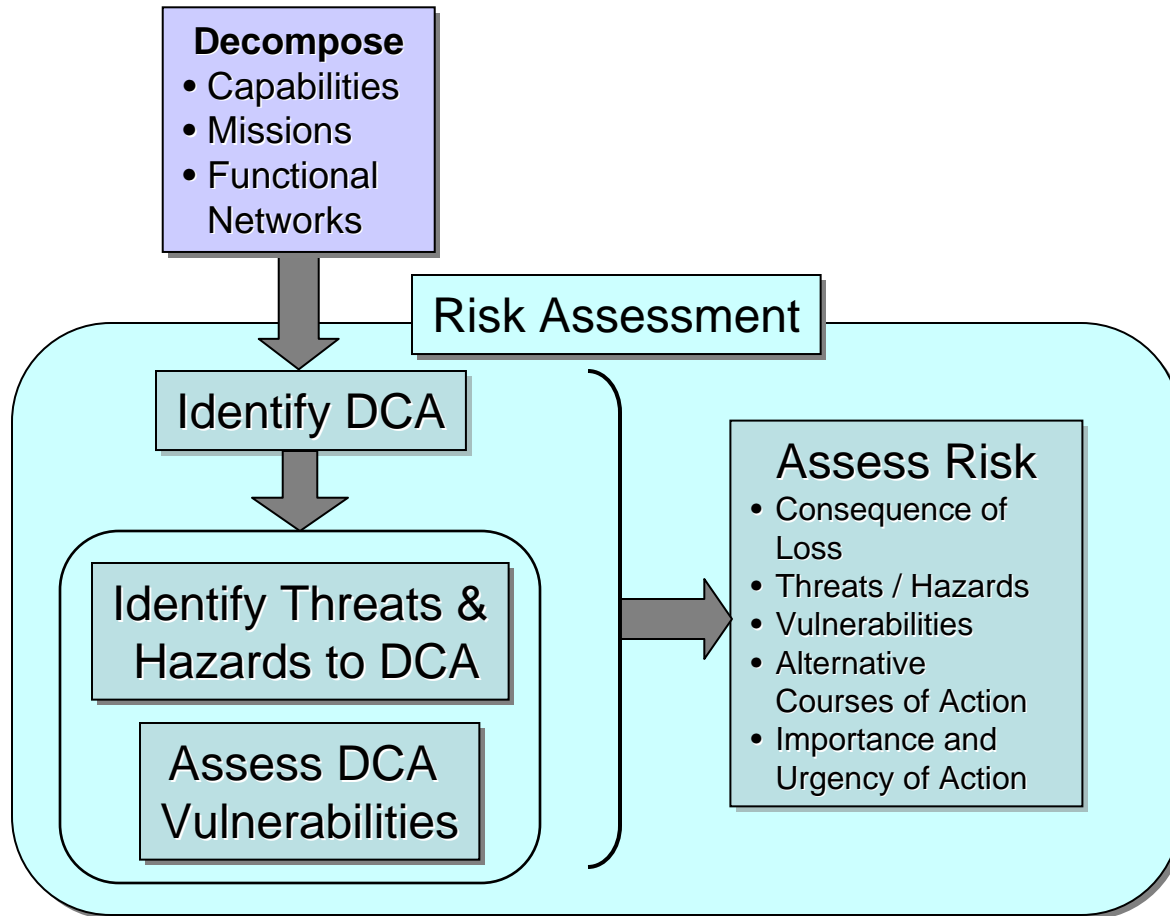
For centralized control all air data flowed through fiber optic lines to allow Baghdad to have a total air picture.

Unfortunately for Saddam, the Iraqi CIP program failed to note that the commercial telephone exchange building these lines all ran through was critical, so there was no backup.



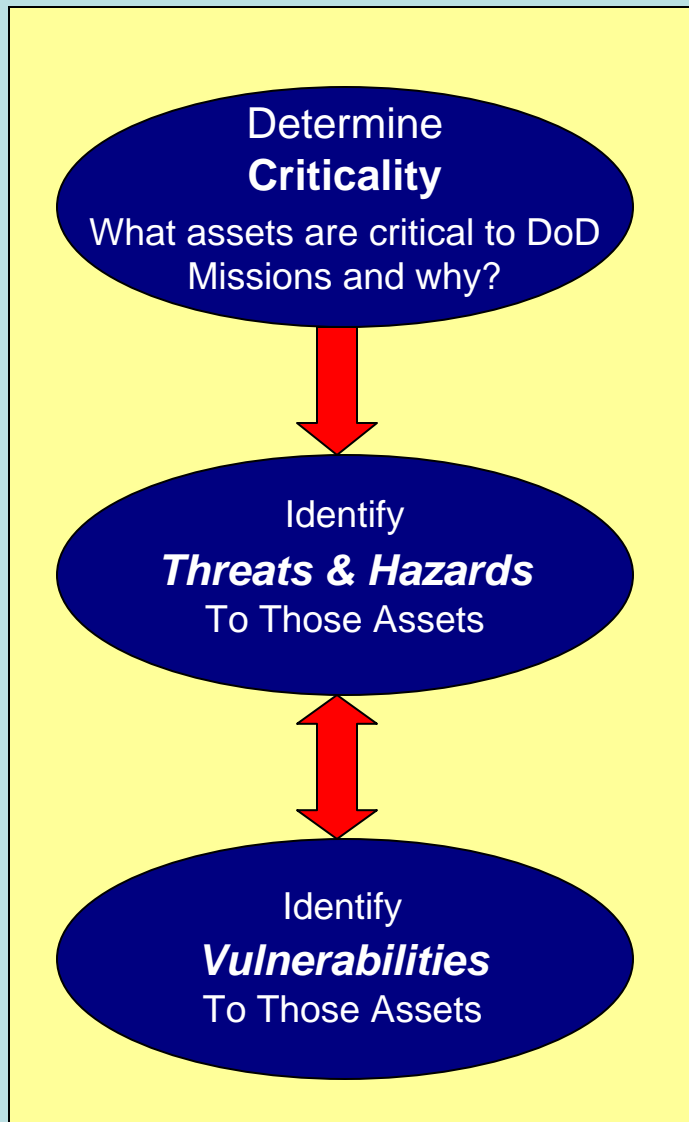
Basic DCIP Process Elements

POLICY



ELEMENTS OF DCIP RISK MANAGEMENT

RISK ASSESSMENT



Make Informed
Risk Management
Decision

RISK RESPONSE



Ongoing Efforts



CRITICALITY



POLICY

Criticality Requirements

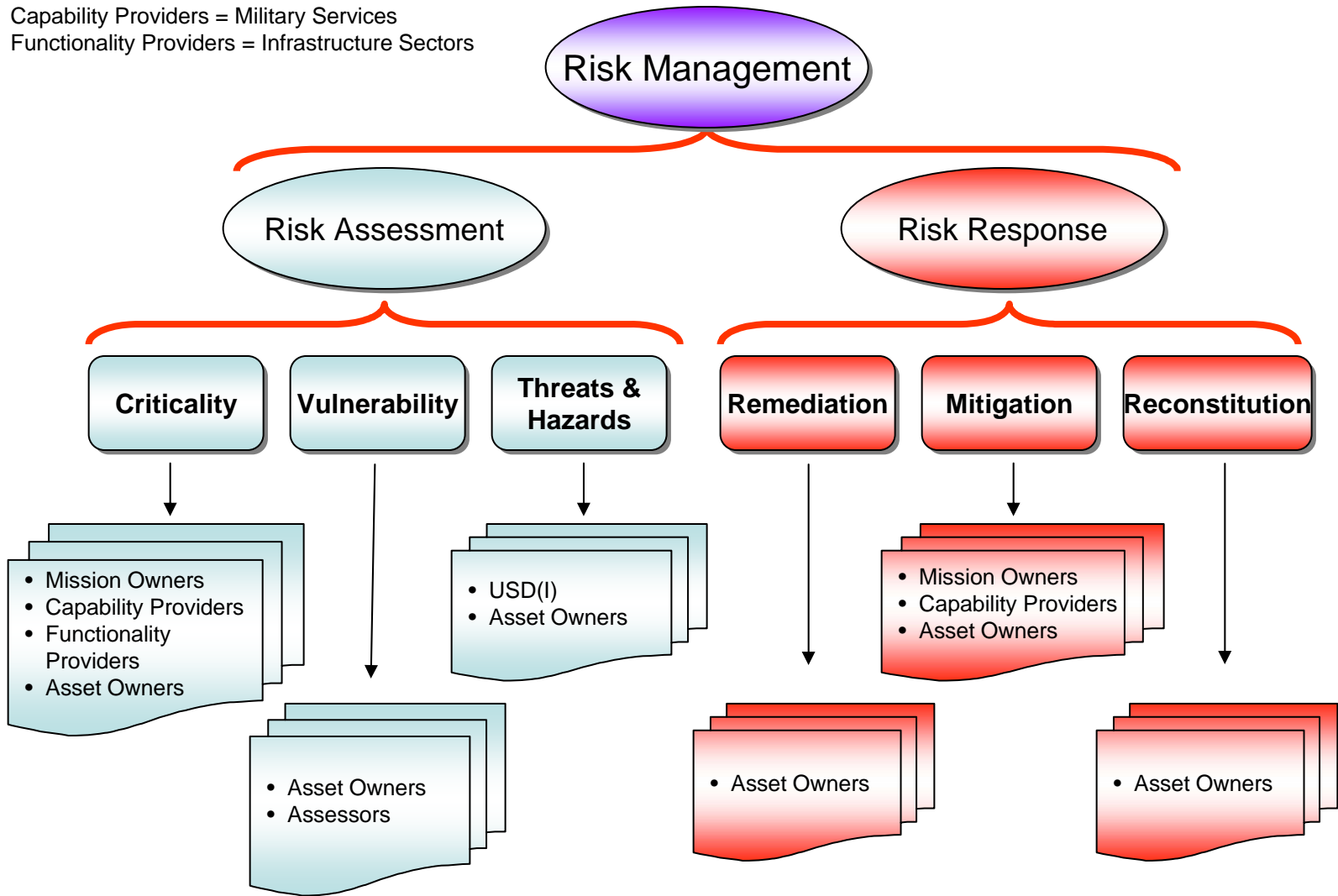
- ❑ HSPD-7 requires identification of critical assets that could:
 - Cause WMD-level health or mass casualty effects
 - Impair ability to perform essential missions or ensure public health and safety - **Basis of DoDD 3020.40**
 - Undermine State or local government capabilities
 - Damage private sector's orderly functioning
 - Have a negative impact on the economy
 - Undermine public morale and confidence in economy or government



DCIP Risk Management Responsibilities

POLICY

Capability Providers = Military Services
Functionality Providers = Infrastructure Sectors





HD&ASA Responsibilities for Criticality

- ❑ DoDD 3020.40 Requirements
 - 5.1.2. Develop and ensure the implementation of DCIP policy and program guidance for the identification, prioritization, and protection of Defense Critical Infrastructure including issuance of strategies and standards.
 - 5.1.9. Integrate all DoD Component DCIP requirements and priorities for critical assets and related vulnerabilities.
- ❑ DoDI 3020.45 Requirements
 - 5.1.1.4. DCA identification across all the DOD Components and defense sectors using a mission-focused process that includes all DOD functions as described in DOD Directive 5100.1.
 - ❑ DCIP Critical Asset Identification Process (CAIP) drafted to replace the Criticality Process Guidance Document (CPGD) to meet the requirements to identify and prioritize DCI.
 - ❑ **HD does not yet have a list of DCAs to prioritize, but can work from the approved TCA list in the event of an incident**



DCIP Community Responsibilities for Criticality

POLICY

- ❑ From DoDD 3020.40
- ❑ COCOMs
 - 5.9.2. Coordinate with the Military Departments, the Defense Agencies, DoD Field Activities, and Defense Sector Lead Agencies identified in subparagraph 5.11.1., to identify and assess critical assets and associated infrastructure interdependencies pertinent to mission accomplishment within assigned regional or functional areas of responsibility.
- ❑ Services
 - 5.10.3. Identify, assess, and document, in coordination with other DoD Components and Defense Sector Lead Agencies identified in subparagraph 5.11.1., critical assets and associated infrastructure dependencies needed to implement required Combatant Command capabilities and other statutory responsibilities.
- ❑ Sectors
 - 5.11.3. Establish and maintain a characterization of the Defense Sector support functions, systems, assets, and dependencies as they relate to operational capabilities and assets identified by the DoD Components.
 - 5.11.5. Plan and coordinate with all DoD Components that own or operate elements of the Defense Sector to identify, analyze, and assess the Defense Sector's critical assets and related mission impacts.
- ❑ From the DODI 3020.45
- ❑ CJCS
 - 5.5.3. Provide to the ASD(HD&ASA), the DOD Components, and DISLAs:
 - 5.5.3.1. An up-to-date list of recommended DCAs
- ❑ COCOMs
 - 5.6.2.1 Coordinate and assist further DOD Component and DISLA analyses of command missions and related capabilities to identify TCAs necessary to execute these capabilities
 - 5.6.2.2. Validate TCAs submitted by the DOD Components as critical to the fulfillment of their mission
- ❑ MILDEPS/USSOCOM/NGB/DA/FA
 - 5.7.1. Identify and OPR to establish, resource, and execute a component program for matters pertaining to the identification, prioritization, assessment, mitigation, remediation, and management of risk to DCI, including the identification and prioritization of Service component METS and required capabilities

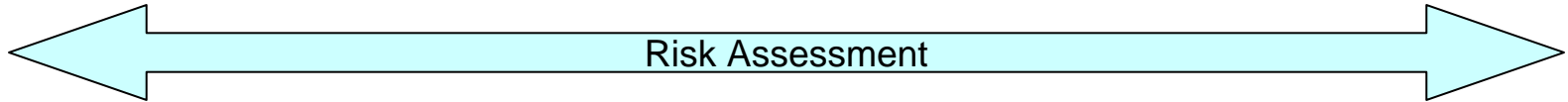


THREAT/HAZARD ASSESSMENTS



Basic DCIP Process Elements

POLICY



Identify Threats & Hazards

USD(I)
direction to
DIA

IC conducts foreign
threats assessment
to DCA(s)

Request for
assessment
of threats to
DCA(s)

CI/LE conducts
domestic threats
assessment
to DCA(s)

USD(I)
direction to
CIFA

Identified
general and
specific
Threats and
Hazards to
DCAs

IC & CI Inform
Authorities
• OASD HD
• Asset Owners
• Mission Owners
• Command Chain

Identified
general and
specific
Threats and
Hazards to
DCAs

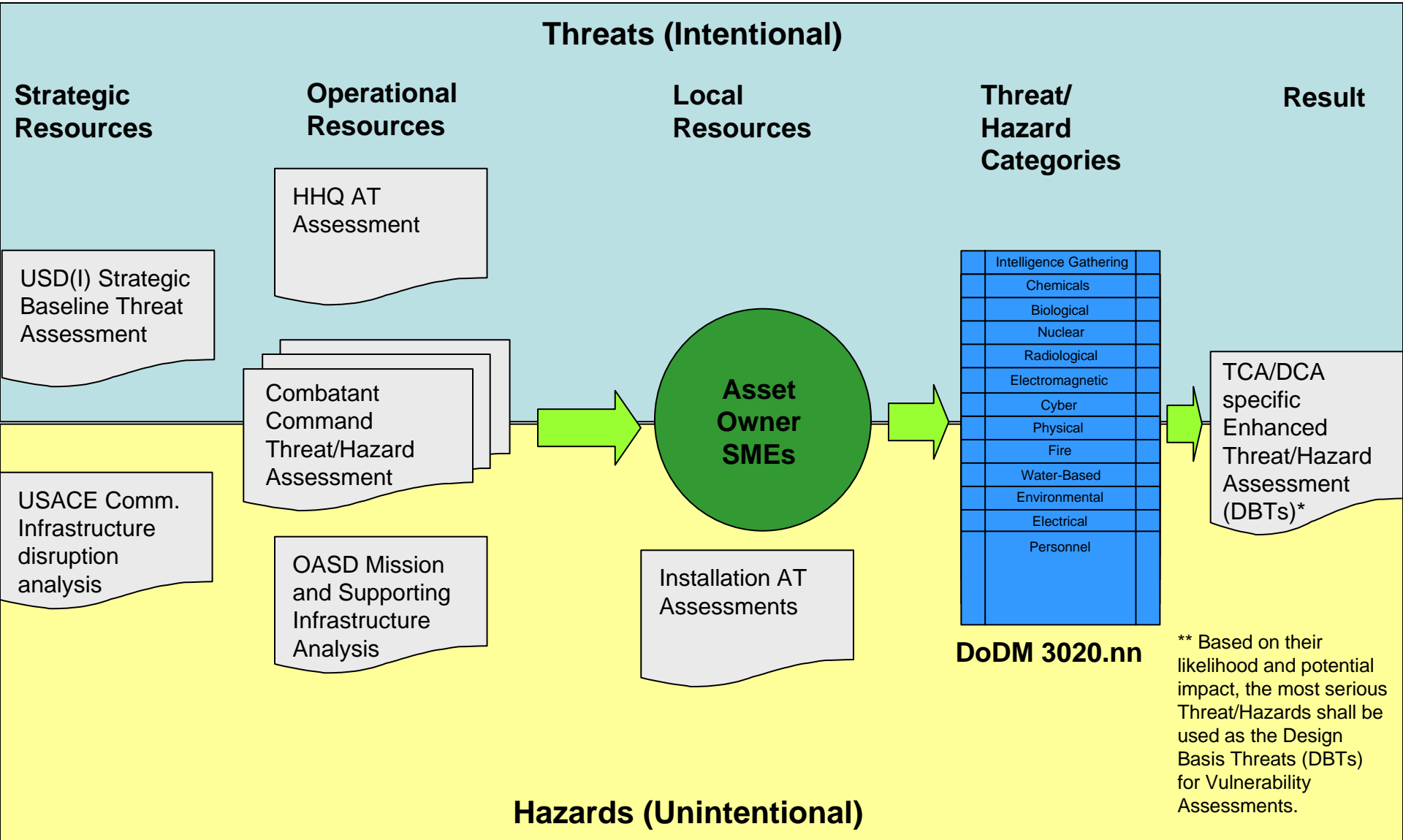
Request IC & CI/LE to
monitor & report threat
changes

Pass to VA Scheduling
• Paired DCAs and
Threats/Hazards



POLICY

Threat & Hazard Assessment Process



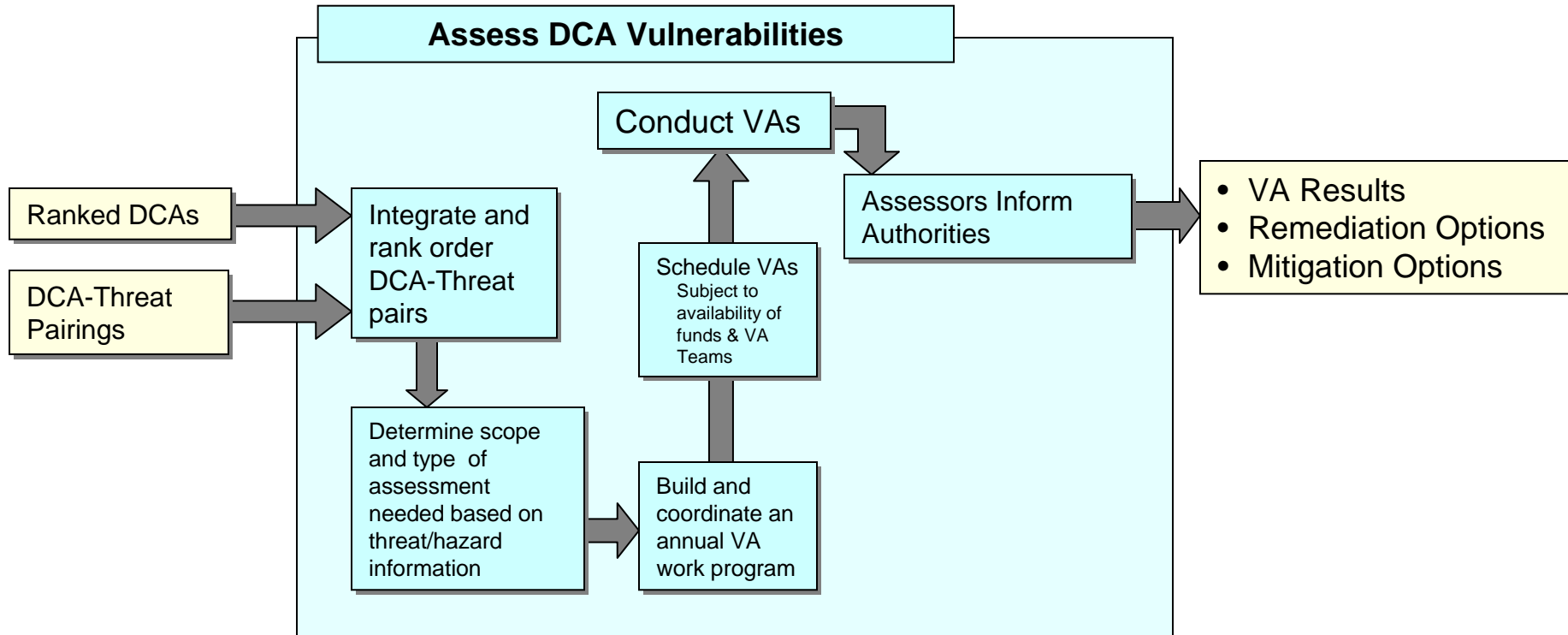
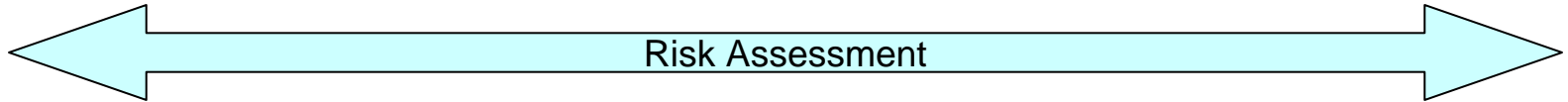


VULNERABILITY ASSESSMENTS



Basic DCIP Process Elements

POLICY





Vulnerability Assessment

POLICY

Pre-Assessment Resources

TCA Physical and Procedural Vulnerabilities

Supporting Infrastructure Physical and Procedural Vulnerabilities

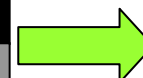
Further Supporting Infrastructure Physical and Procedural Vulnerabilities

Define the support the TCA provides the mission

CRITICALITY

Identify the likely Design Basis Threats for this TCA

THREAT/HAZARD



Identify Mission Failure Vulnerabilities of the TCA

Identify Mission Degradation Vulnerabilities of the TCA

Identify Mission Failure Vulnerabilities of the Supporting Infrastructure

Identify Mission Degradation Vulnerabilities of the Supporting Infrastructure

Identify Mission Failure Vulnerabilities of the Supporting Infrastructure

Identify Mission Degradation Vulnerabilities of the Supporting Infrastructure

Etc.

Supporting Infrastructure:

Power:

Electricity
POL
NG

Communications:

Voice
Data

Transportation:

Air
Maritime
Rail
Road

Other:

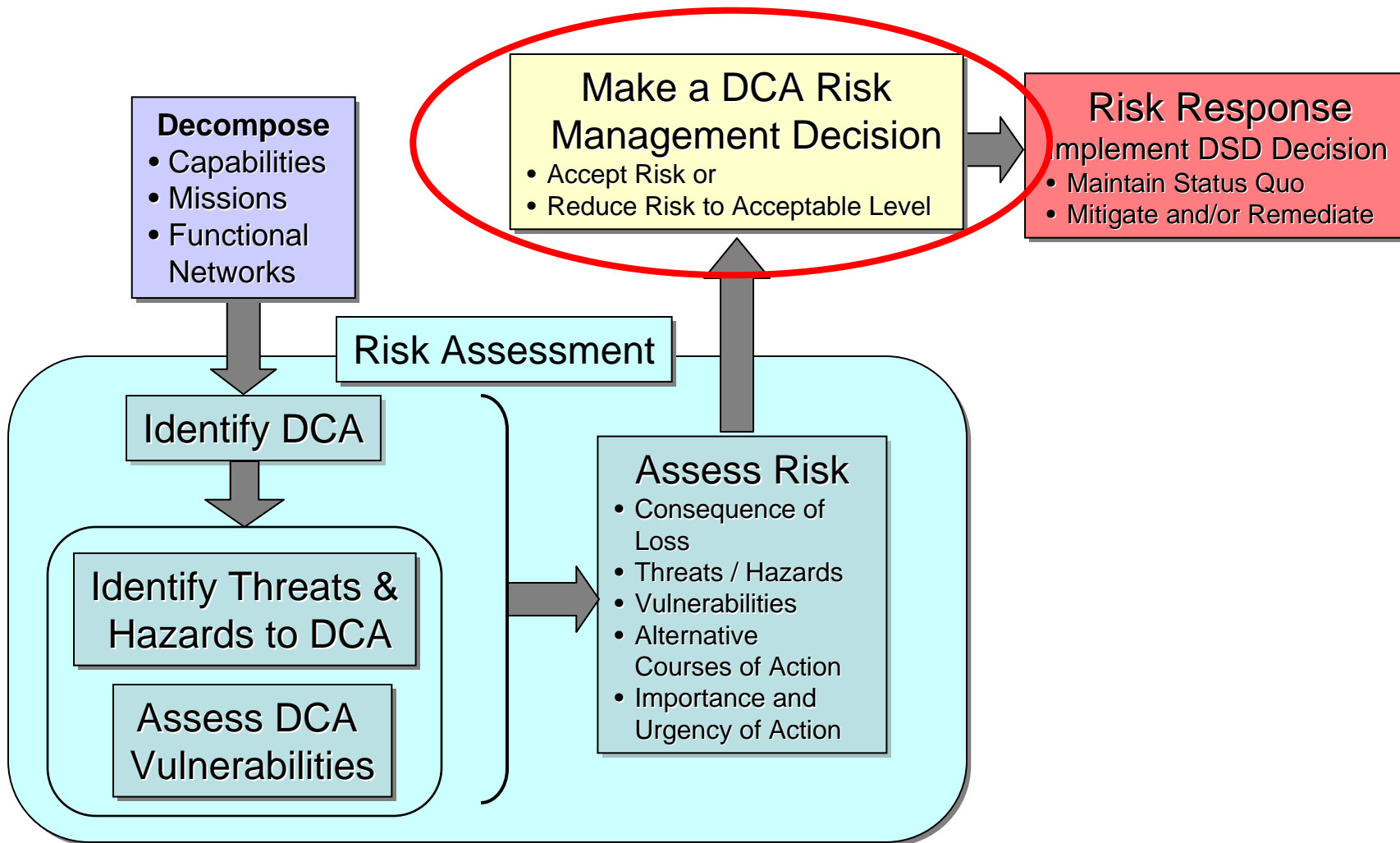
Water
Wastewater
HVAC
Chemicals



RISK DECISION & RESPONSE



Basic DCIP Process Elements





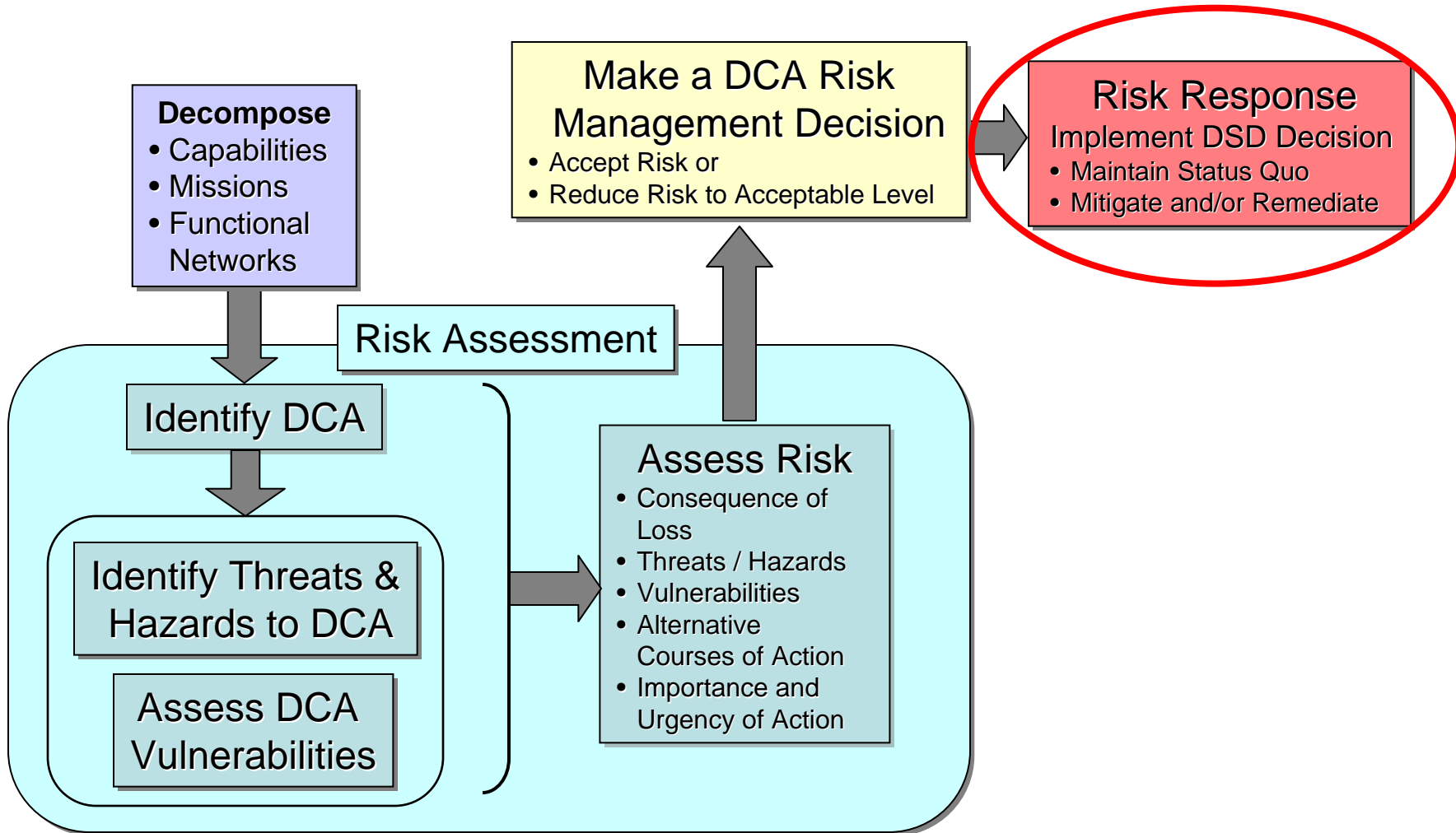
POLICY

Effective Risk Management Decision-Making Activities

- ❑ Effective risk management decision-making activities must include:
 - Determining which *risk response options* are most appropriate in a given situation and the most *cost effective means* for reducing risk to an acceptable level
 - Determining the *priority* for a given risk response relative to other projects that impact a *specific mission*
 - Determining the priority for a given risk response relative to all other DCIP *risk management measures* that impact DoD's ability to execute the National Military Strategy



Basic DCIP Process Elements





DCA Risk Decision Package

CORRESPONDENCE

- OSD prepares “correspondence”
- Chops from OSD PSAs, DCA owner, MILDEPSECs and DJS

DCA RISK DECISION PACKAGE

Executive Summary (3 pages)

- OSD prepares

Attachment A – Risk Assessment

- DCA owner documents
- Narrative w/ supporting numbers

Attachment B – Detailed Risk Reduction Alternatives Considered

- DCA owner prepares; chops by DJS, DISLA(s)

Attachment C – DCA Consequence of Loss

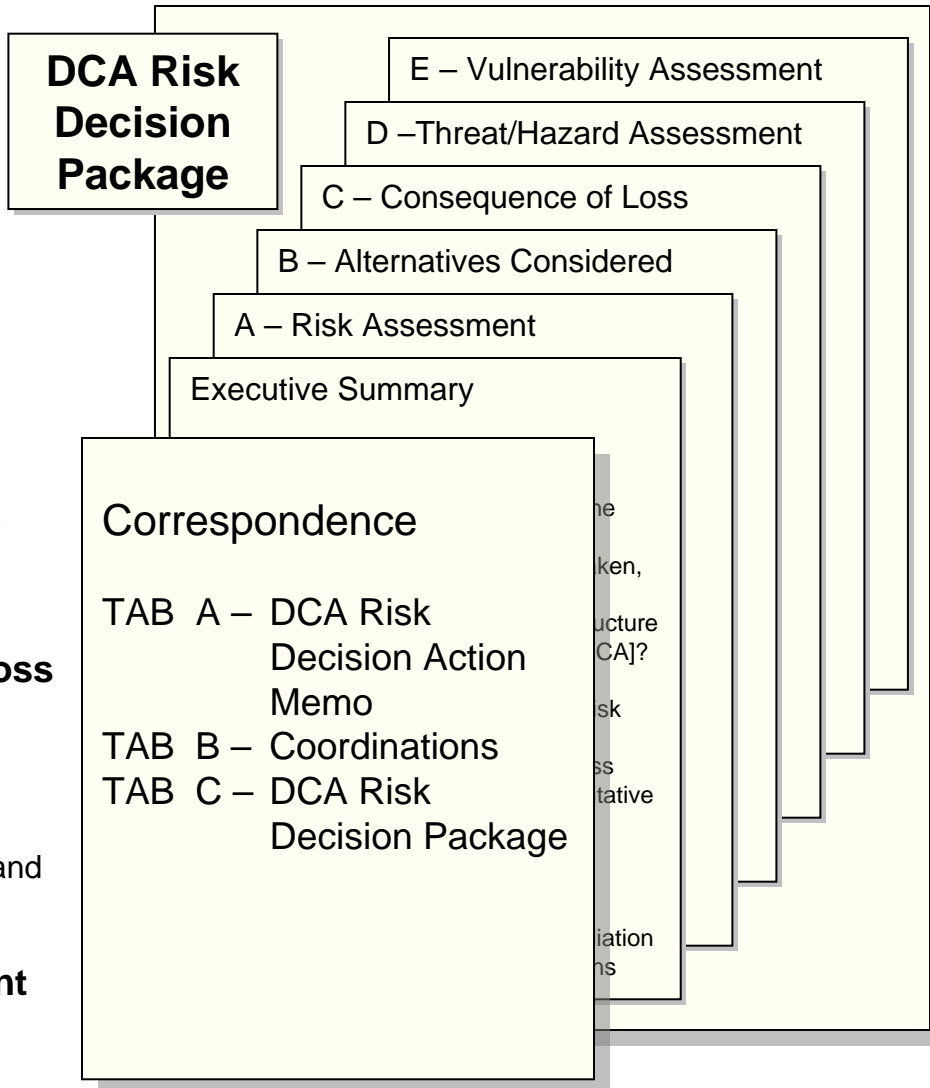
- DCA owner prepares; chop by DJS, MILSEC or PSA
- Narrative w/ supporting numbers

Attachment D -- Threats//Hazards

- DCA owner prepares; chop by USD(I), and USD(AT&L) or possibly USD(NII)
- Narrative format

Attachment E – Vulnerability Assessment

- DCA owner prepares
- Narrative and supporting numbers





DCIP Risk Response Options

POLICY

- Accept Risk**

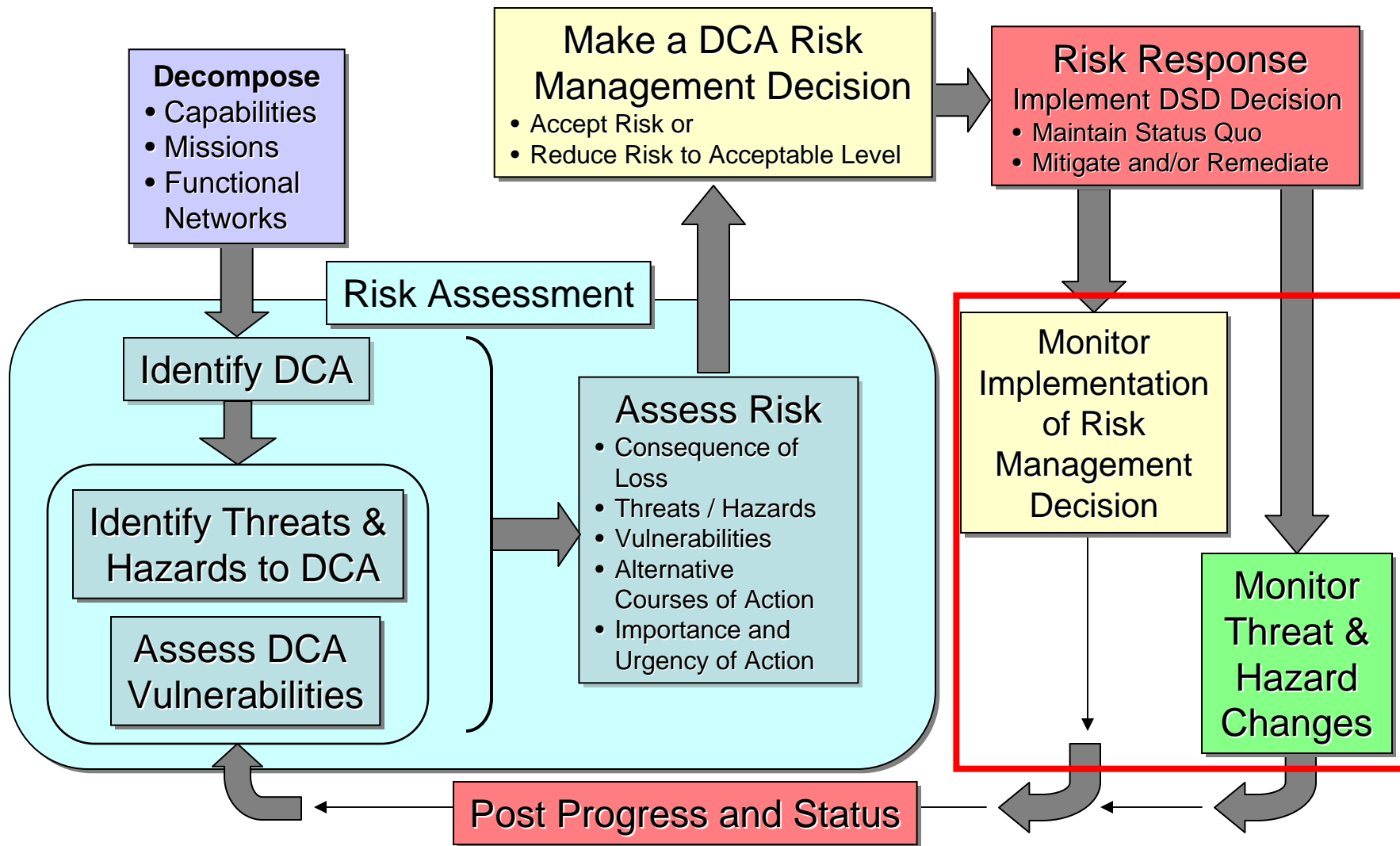
- Mitigate Potential Threats & Hazards (Minimize the effect)**
 - Change Tactics, Techniques, or Procedures
 - Add Redundancy
 - Select Alternate Ways to Perform Functions
 - Isolate or Harden Identified Critical Assets
 - Physically Guard Previously Unprotected Assets

- Remediate Vulnerabilities**
 - Remediation Planning should include a full range of doctrine, organization, training, material, leadership, and education, personnel, and facilities (DOTMLPF) options

- Reconstitute Lost Capability**



Basic DCIP Process Elements





QUESTIONS?



BACK UP SLIDES