DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DISA Task Critical Asset Nomination Process

Fred P. Ruonavar

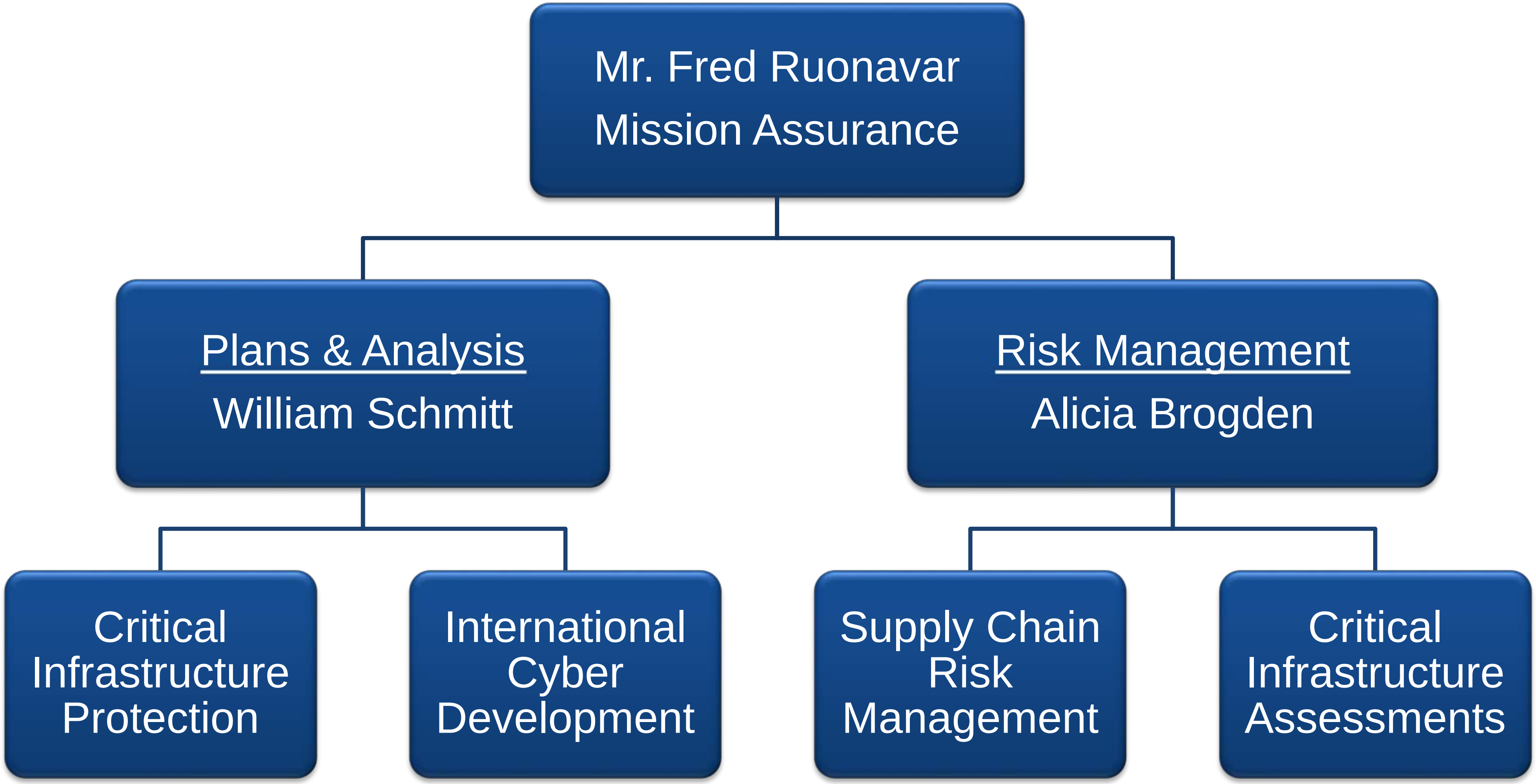
Chief, DISA Mission Assurance & DISA/DoDIN

Critical Infrastructure Protection (CIP) Program

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

DoDIN/DISA Mission Assurance (MA) Branch Organizational Chart



Mr. Fred Ruonavar
Mission Assurance

Plans & Analysis
William Schmitt

Risk Management
Alicia Brogden

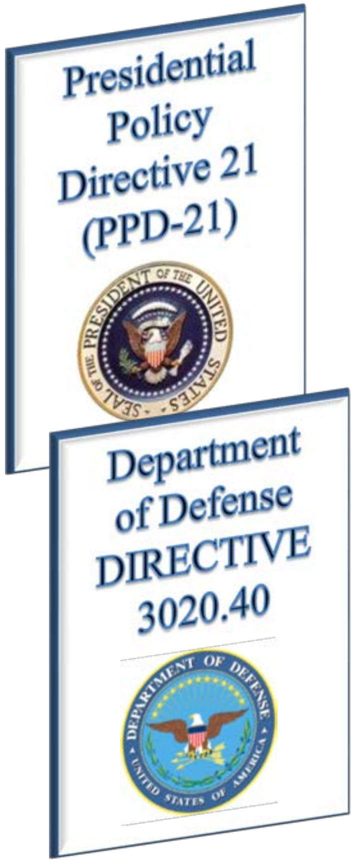
Critical Infrastructure Protection

International Cyber Development

Supply Chain Risk Management

Critical Infrastructure Assessments

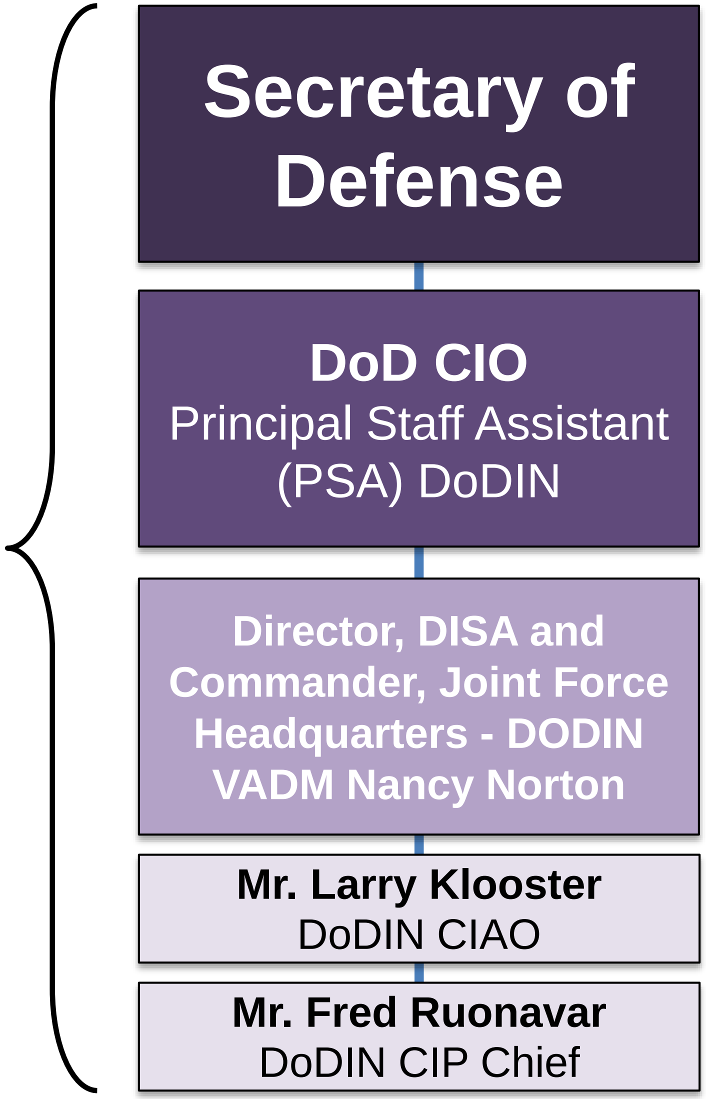
DoDIN CIP Authority



Presidential Policy Directive 21 (PPD-21)

Department of Defense DIRECTIVE 3020.40

- **Presidential Policy Directive 21 (PPD-21):** identifies responsibilities for Federal Departments and Agencies.
- **Department of Defense Directive (DoDD) 3020.40** establishes policy and assigns DoD CIO as PSA for DoDIN Sector, Mission Assurance and Critical Infrastructure Protection.



Secretary of Defense

DoD CIO
Principal Staff Assistant (PSA) DoDIN

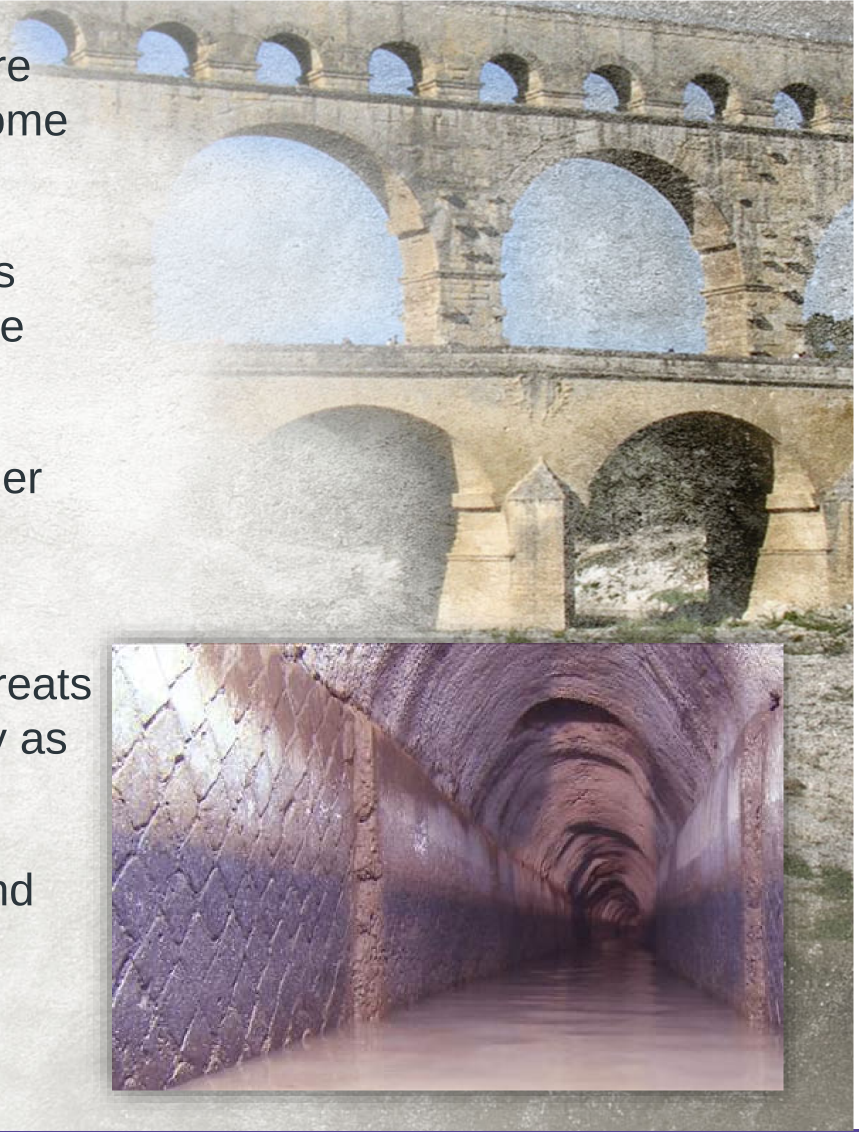
Director, DISA and Commander, Joint Force Headquarters - DODIN VADM Nancy Norton

Mr. Larry Klooster
DoDIN CIAO

Mr. Fred Ruonavar
DoDIN CIP Chief

Ancient Critical Infrastructure Protection

- Romans began developing critical infrastructure such as roads, food stores, and aqueducts (some Roman aqueducts still in use to this day).
- Realizing their importance, Trajanus Hadrianus Augusts enacted laws to specifically protect the aqueduct system.
- Built first aqueduct entirely underground in order to conceal and protect it from enemies, and to protect from erosion and deterioration.
- Initially the Romans were very aware of the threats they faced and built infrastructure with security as the prime element.
- Over time the Romans became complacent and focused more on aesthetics vice security.
- **There are similar parallels today…**

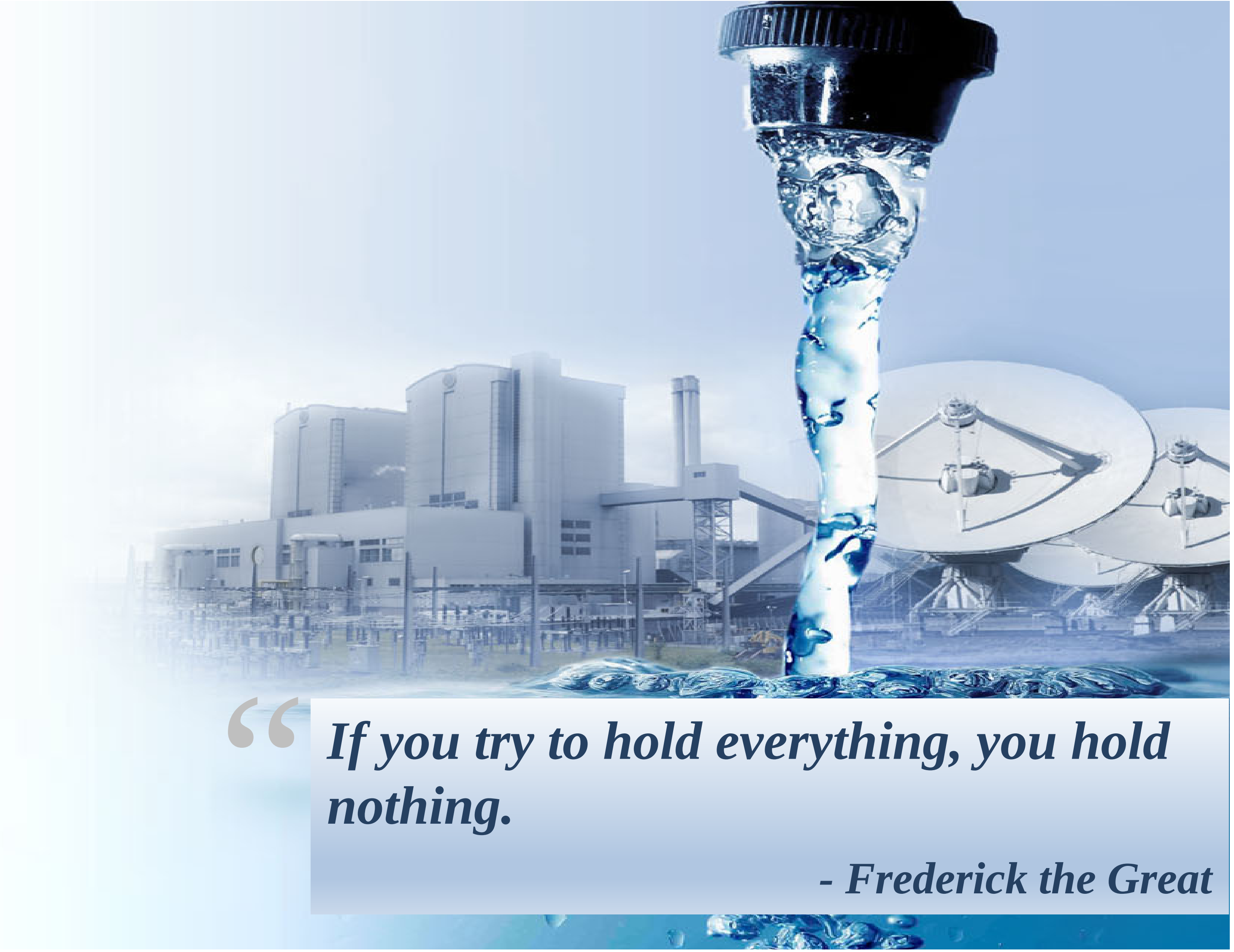


Mission Assurance

What is Critical?

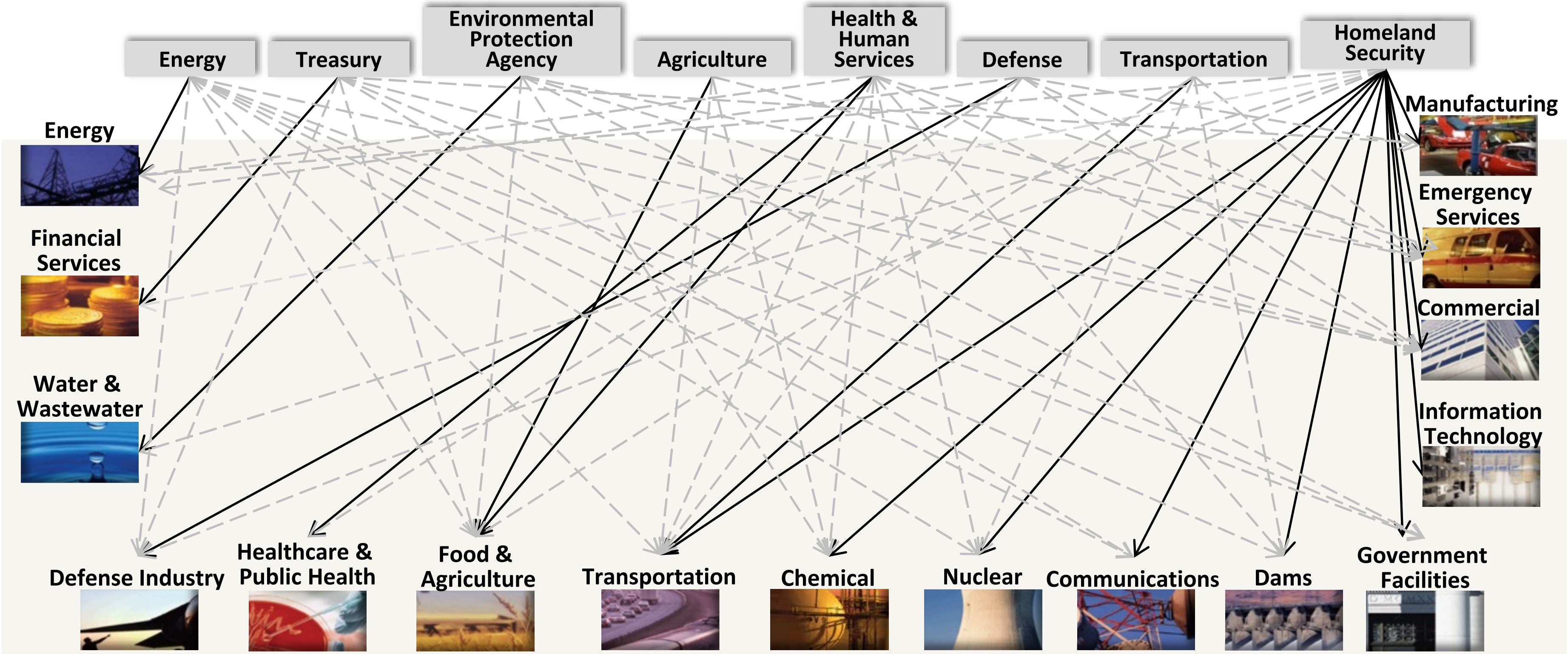
Mission Analysis

- What must we be able to do?
- What are the T1 support plans?
- What phase of operation are we in?
- What assets are required?
  - How many tanks, ships, planes
    - What type of C2 is required?
    - What's the bandwidth required
    - What's the next requirement?
- What do those assets rely on?
    - Who are the vendors?
    - What does their infrastructure look like?
    - What are their interdependencies?



> *"If you try to hold everything, you hold nothing.*
>
> *- Frederick the Great*

“Whole of Government” Responsibility



Infrastructure sectors are connected at multiple points through a wide variety of mechanisms, such that a bi-directional relationship exists between the functional states of any given pair of infrastructures.

Why it matters…

Size of the Active Force

1.4 Million

Deployed Operations

- *130K(+) Troops*
- *150(+) countries*

Partner Nations

- *60(+) Allies*
- *180(+) Partnerships*

Warfighting Domains

- *Air*
- *Land*
- *Maritime*
- *Cyber*

~15,000 Applications

Task Critical Asset (TCA) Nomination

The Department of Defense (DOD) relies on a global network of defense critical infrastructure so essential that the incapacitation, exploitation, or destruction of an asset within this network could severely affect DOD's ability to deploy, support, and sustain its forces and operations worldwide and to implement its core missions. Because of its importance to DOD operations, this defense critical infrastructure could be vulnerable to attacks by adversaries, and vulnerable to natural disasters and hazards, such as hurricanes and earthquakes.

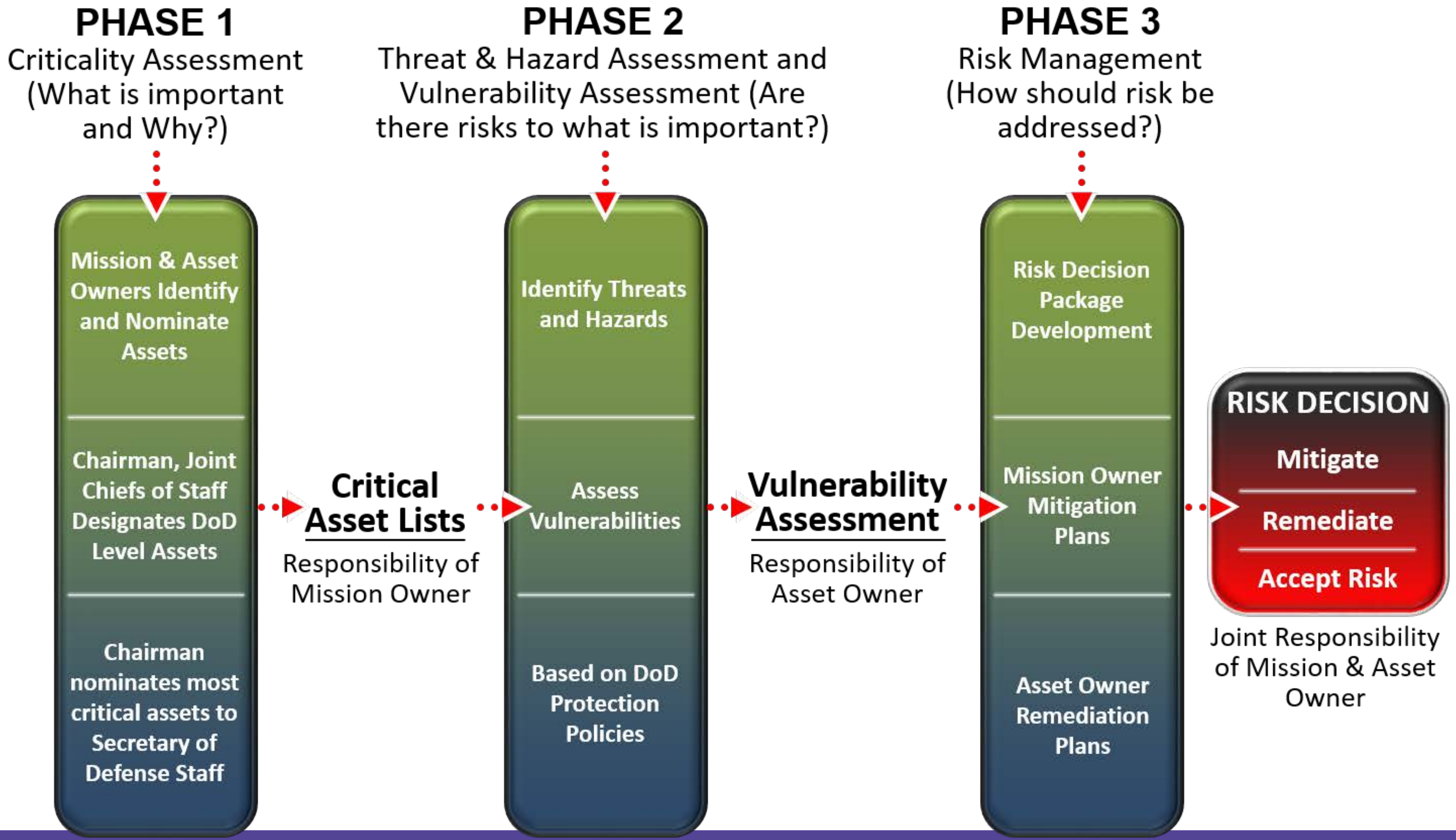
What are TCAs?

- **Tier 1 Task Critical Assets** are assets of such extraordinary importance that their incapacitation or destruction would have a serious, debilitating effect on the ability of one or more military services, combatant commands, or DCIP Defense Infrastructure Sector Lead Agents to execute the mission essential tasks they support.
- **Tier 2 Task Critical Assets** are defined as causing severe mission (or function) degradation if the asset is lost, incapacitated, or disrupted.
- **Defense Critical Assets** are the assets most critical for fulfilling overall DOD missions and are identified from the universe of Task Critical Assets.

Mission Essential Tasks (METLs) => Task Critical Assets (TCAs) => Defense Critical Assets (DCAs)

DoD’s Mission Assurance Process

DoDD 3020.40



PHASE 1
Criticality Assessment (What is important and Why?)

- Mission & Asset Owners Identify and Nominate Assets
- Chairman, Joint Chiefs of Staff Designates DoD Level Assets
- Chairman nominates most critical assets to Secretary of Defense Staff

Critical Asset Lists
Responsibility of Mission Owner

PHASE 2
Threat & Hazard Assessment and Vulnerability Assessment (Are there risks to what is important?)

- Identify Threats and Hazards
- Assess Vulnerabilities
- Based on DoD Protection Policies

Vulnerability Assessment
Responsibility of Asset Owner

PHASE 3
Risk Management (How should risk be addressed?)

- Risk Decision Package Development
- Mission Owner Mitigation Plans
- Asset Owner Remediation Plans

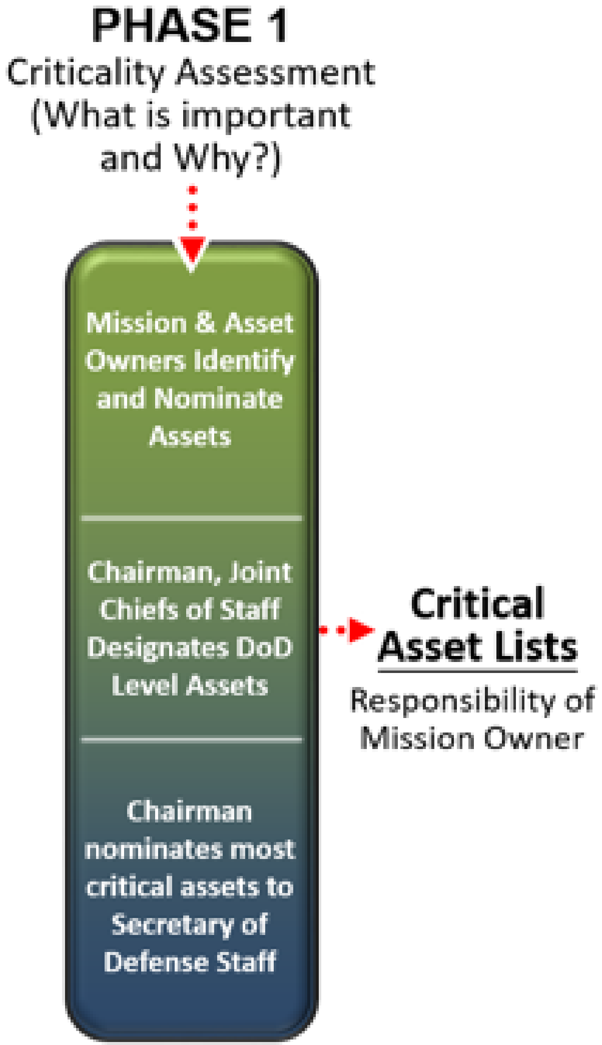
RISK DECISION

- Mitigate
- Remediate
- Accept Risk

Joint Responsibility of Mission & Asset Owner

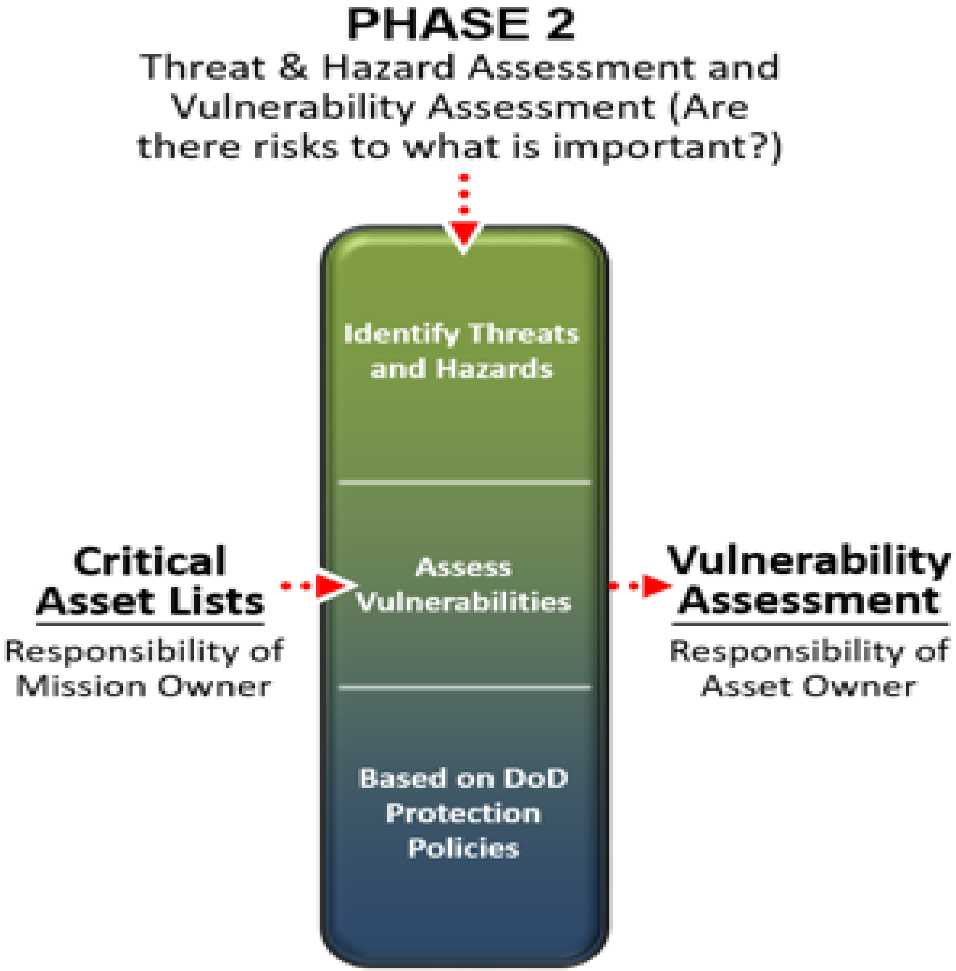
Phase I – What is important and Why?

- Input:
  - Mission analysis and plan decomposition
  - Asset analysis
    - Mission Essential Tasks (MET)
    - Asset interaction
    - Asset dependencies
- Decisions:
  - Commanders determine asset criticality
- Output:
  - Critical Asset Lists (TCA, DCA, etc.)


PHASE 1
Criticality Assessment
(What is important and Why?)
Mission & Asset Owners Identify and Nominate Assets
Chairman, Joint Chiefs of Staff Designates DoD Level Assets
Chairman nominates most critical assets to Secretary of Defense Staff
Critical Asset Lists
Responsibility of Mission Owner

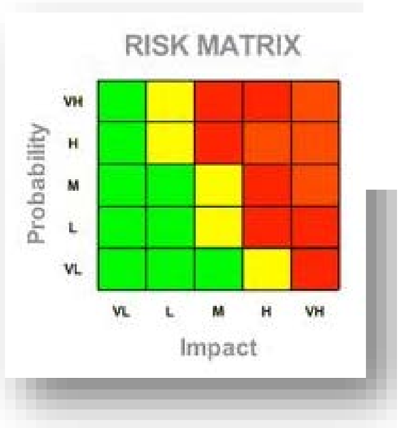
Phase 2 – Are there risks to what is important?

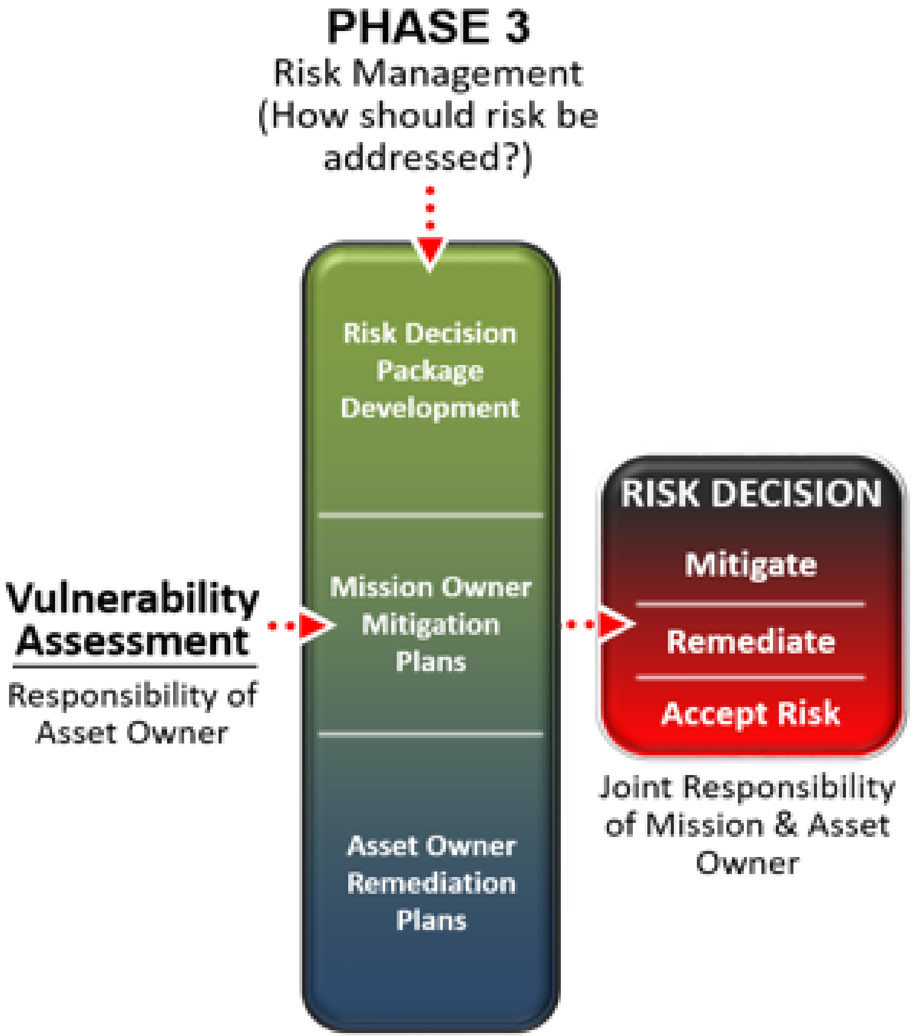
- Input:
  - Critical Asset Lists
  - Threat Intelligence
  - Vulnerability Identification/Reports
- Decisions:
  - Vulnerability and Risk Determination
- Output:
  - Vulnerability Assessment


PHASE 2
Threat & Hazard Assessment and Vulnerability Assessment (Are there risks to what is important?)
Identify Threats and Hazards
Assess Vulnerabilities
Based on DoD Protection Policies
Critical Asset Lists
Responsibility of Mission Owner
Vulnerability Assessment
Responsibility of Asset Owner

Phase 3 – How should risk be addressed?

- Input:
  - Vulnerability Assessments
  - Resource Availability
- Decisions:
  - Risk Prioritization
  - Resource Obligation
- Output:
  - Risk Decision Package
  - Risk Mitigation Plan





PHASE 3
Risk Management
(How should risk be addressed?)

Vulnerability Assessment
Responsibility of Asset Owner

Risk Decision Package Development

Mission Owner Mitigation Plans

Asset Owner Remediation Plans

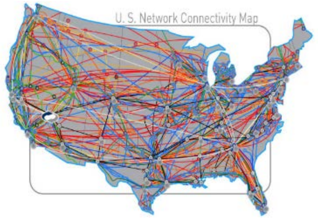
RISK DECISION
Mitigate
Remediate
Accept Risk

Joint Responsibility of Mission & Asset Owner

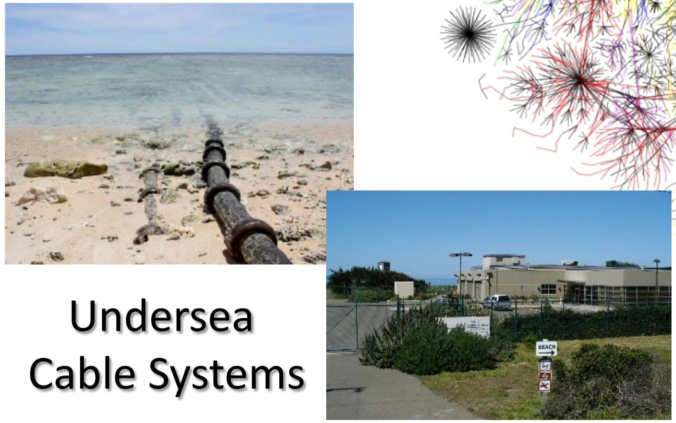
$$\text{Risk} = \frac{((\text{Means} + \text{Motive}) \text{ X Opportunity}) \text{ X Impact}}{\text{Controls}}$$

Internet Visualization

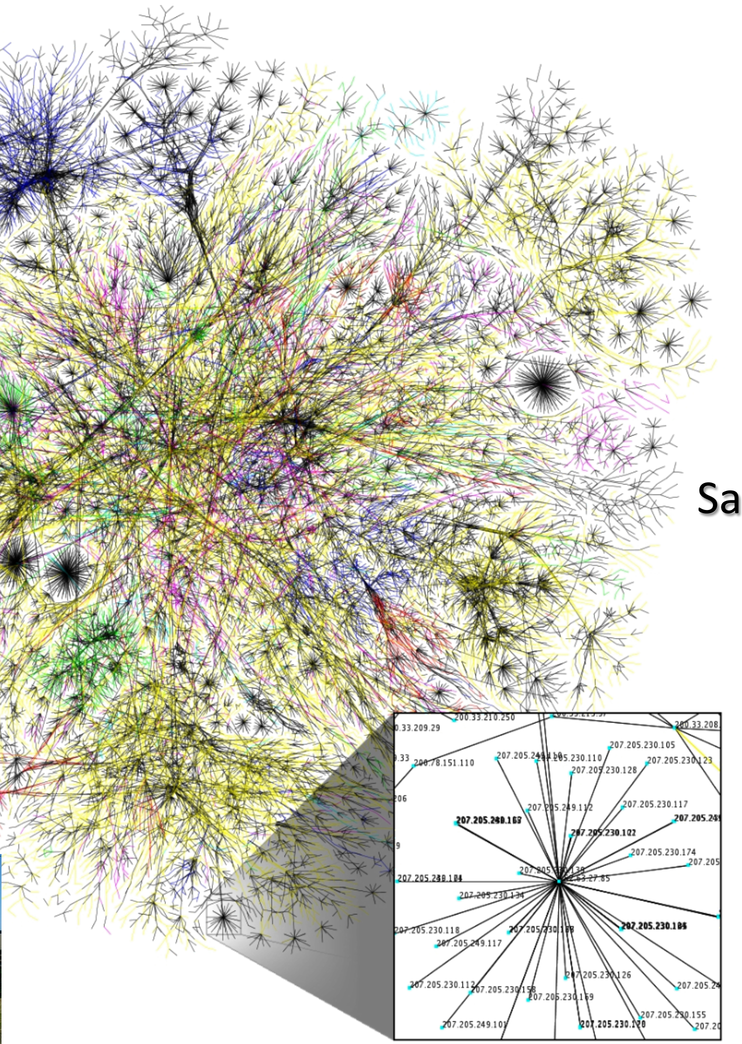
Data Warehouses



Overland Cable Systems



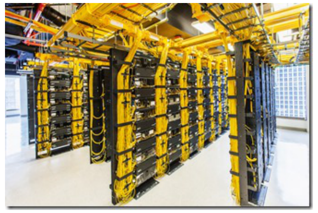
Undersea Cable Systems



Discrete Networks

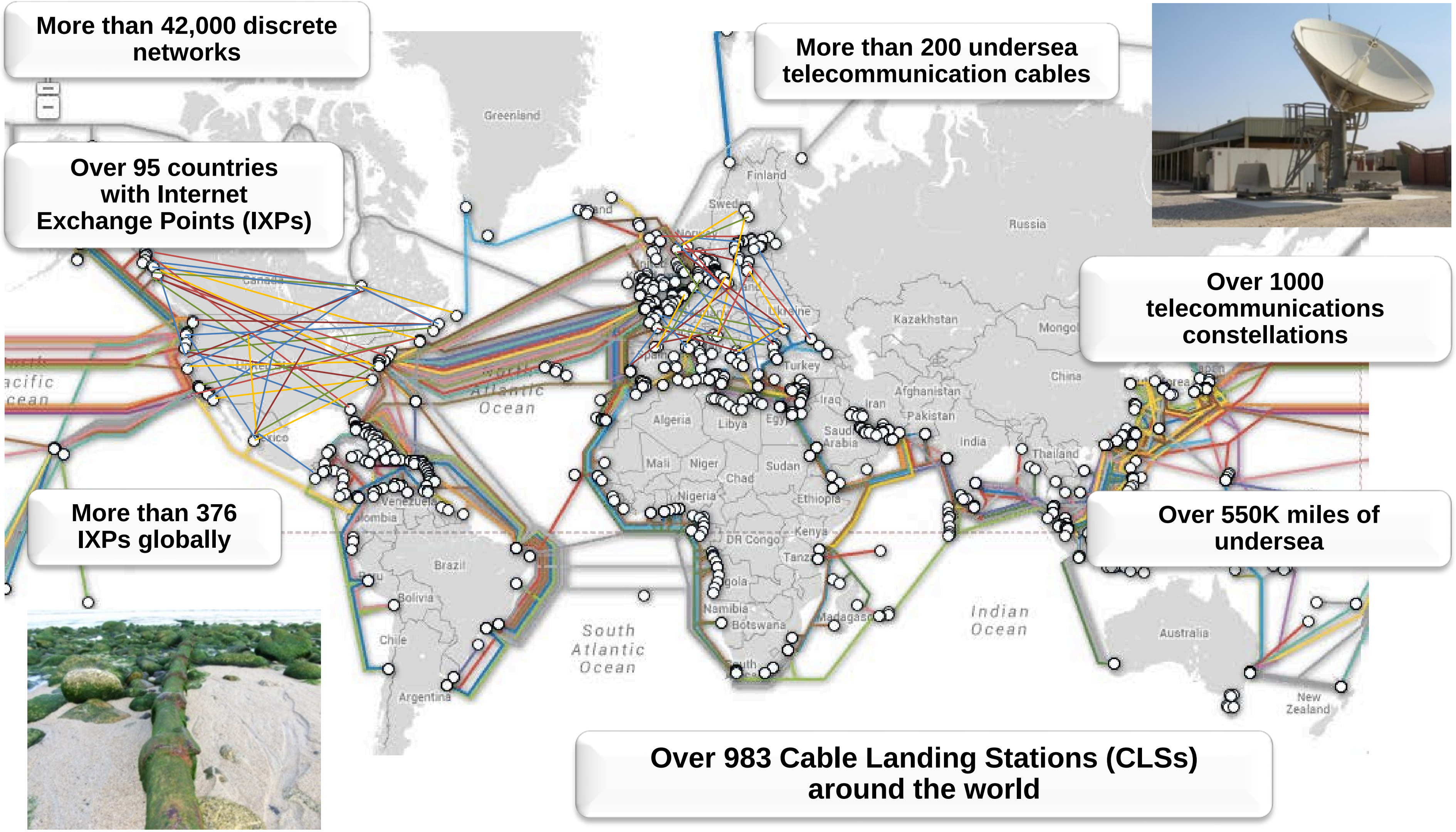
Constellations

Satellite Earth Station



Internet Exchanges

Commercial Telecommunications and the Real Internet



More than 42,000 discrete networks

More than 200 undersea telecommunication cables

Over 95 countries with Internet Exchange Points (IXPs)

Over 1000 telecommunications constellations

More than 376 IXPs globally

Over 550K miles of undersea

Over 983 Cable Landing Stations (CLSs) around the world

Undersea Communications Cables

Carrying 97% of all global communication traffic in 2015, undersea cables are critical to international trade and commerce. The United States supports measures which ensure secure and uninterrupted service along undersea cables

  - More than 1 million km of undersea cable installed globally
  - Last year only 3% of global communications were carried via satellite
  - Widespread disruption to undersea cables would cost the U.S. and its allies billions of dollars

- Despite protection measures undersea cables are susceptible to breaking through fishing, anchoring, deliberate attack, component failure, and natural disasters (i.e., earthquakes, typhoon, etc.)
  - State actors may be looking for vulnerabilities in U.S. and allied undersea cables
  - Landing station and cable locations are publically available
  - Vast majority of breaks occur in shallow water, less than 1000m
  - There are less than two faults a year in deep water, greater than 1000m
  - Law enforcement might not know the threat or the criticality of these systems

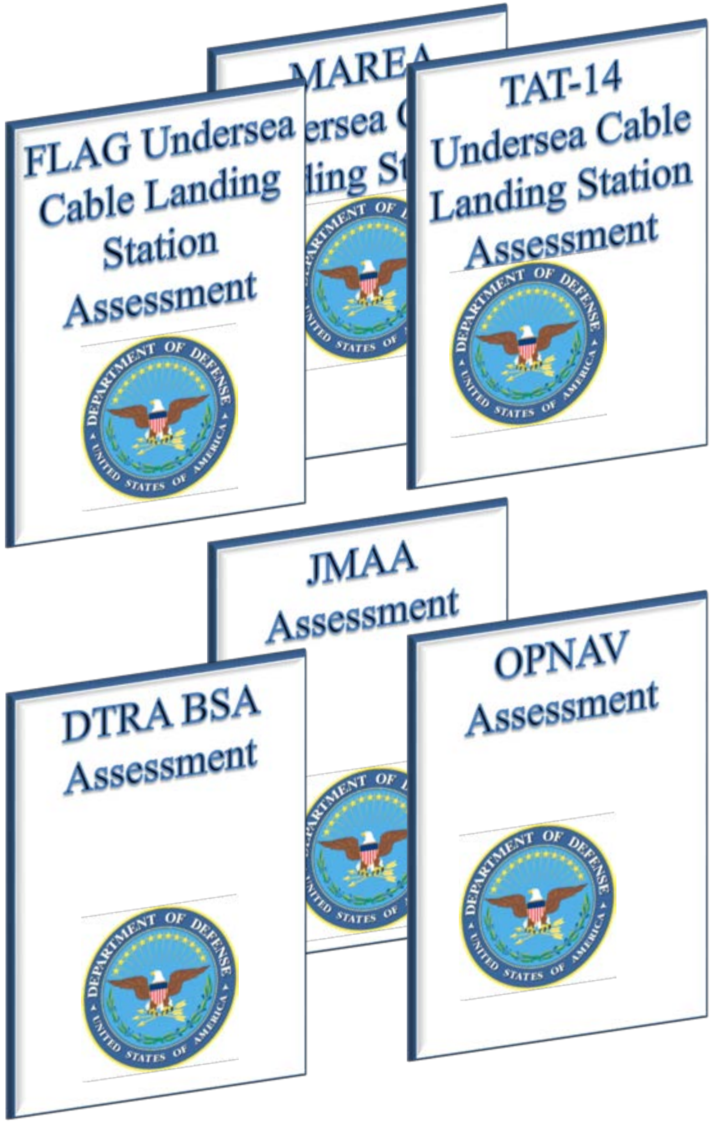
Facts Policy Makers Need to Know Regarding Undersea Cables

- Each Undersea Cable Systems is generally owned by consortia of 4-30 private companies or occasionally a single company
  - 99% of undersea cable systems are non-government owned
- Undersea Cable Systems are not “flagged” to any one Nation State
- The Undersea Cable industry has established Mutual Maintenance Zones and Private Maintenance Agreements around the world, each equipped with dedicated vessels to enable rapid repair.
- Cable repair is organized regionally by private contract - not by government mandate. Contracts require repair ships to sail within 24 hours
- Cable repairs are urgent not only to restore service, but because each cable acts as the backup for other cables

Facts Policy Makers Need to Know Regarding Undersea Cables

- According to the International Cable Protection Committee (ICPC), **there are 56 registered cable ships in the world.** Some are dedicated to cable laying, others are multi-purpose – laying, repair, marine power, oil and gas field work, etc.
- Cable ships are expensive, custom built, require specialized crews, and fly diverse flags (UK, France, Marshall Islands, Singapore, Japan, China, Korea, UAE, Indonesia)
- About half of the ships are on stand-by and half laying new cables or other tasks like training and maintenance

DoDIN/DISA Mission Assurance (MA) Branch
Critical Infrastructure Protection (CIP) Program Assessments



MAREA
ersea C
ling St

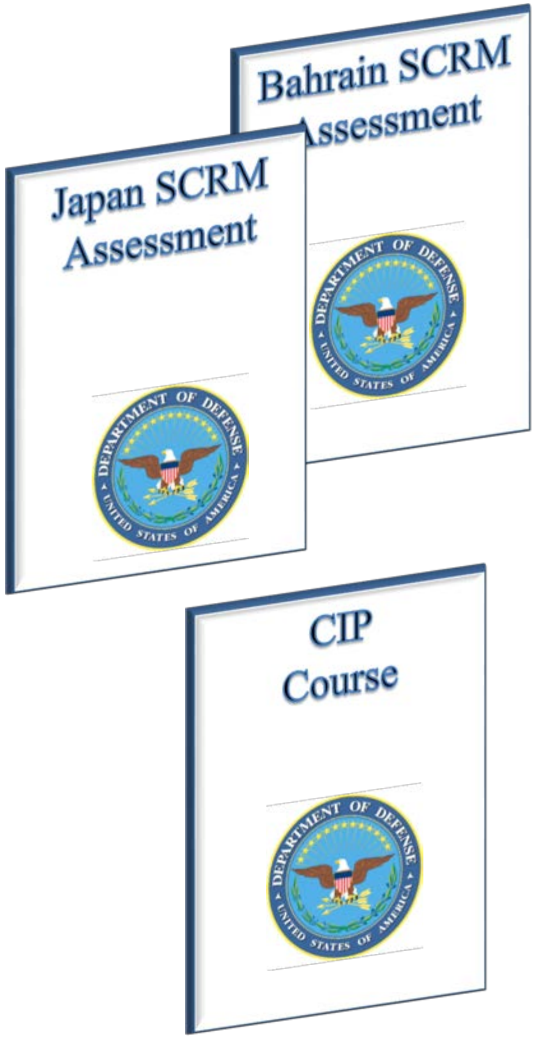
FLAG Undersea Cable Landing Station Assessment

TAT-14 Undersea Cable Landing Station Assessment

JMAA Assessment

DTRA BSA Assessment

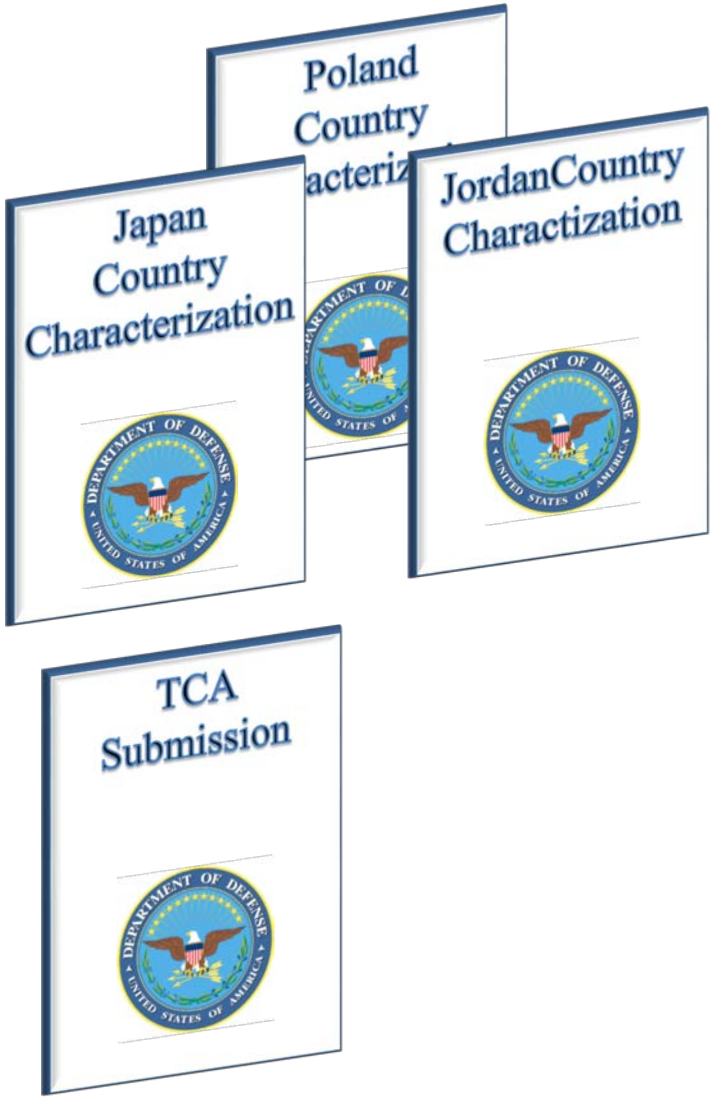
OPNAV Assessment



Bahrain SCRM Assessment

Japan SCRM Assessment

CIP Course



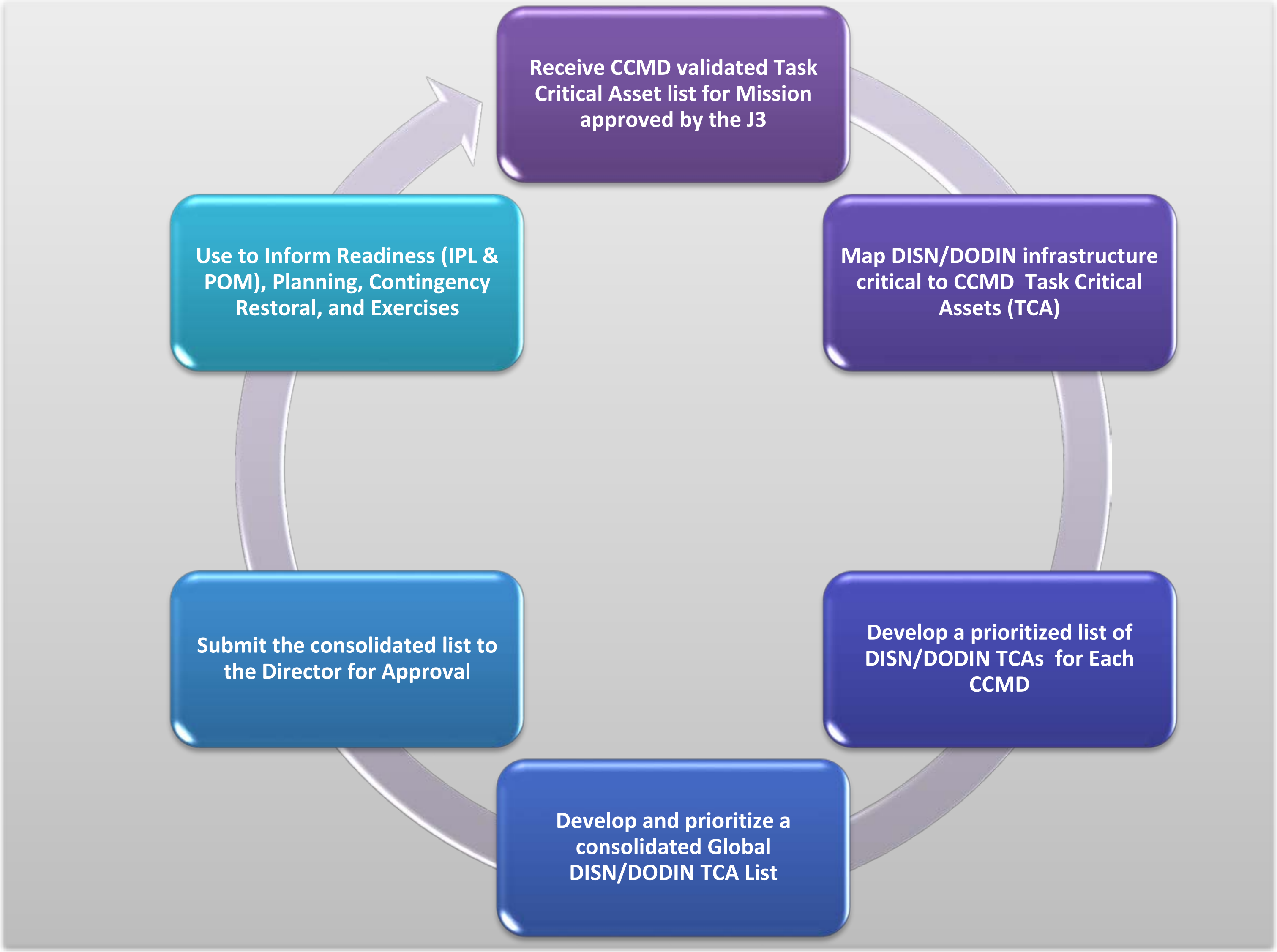
Poland Country
acteriz

Japan Country Characterization

JordanCountry Charactization

TCA Submission

DISA TCA Validation Process



Receive CCMD validated Task Critical Asset list for Mission approved by the J3

Map DISN/DODIN infrastructure critical to CCMD Task Critical Assets (TCA)

Develop a prioritized list of DISN/DODIN TCAs for Each CCMD

Develop and prioritize a consolidated Global DISN/DODIN TCA List

Submit the consolidated list to the Director for Approval

Use to Inform Readiness (IPL & POM), Planning, Contingency Restoral, and Exercises

Questions

rate us

take the 3-question survey available on the AFCEA 365 app

visit us

DISA Booth # 443

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**