# United States Coast Guard Cyber Command

## Achieving Cyber Security Together

Brett Rouzer
Chief of MCIKR Protection
U.S. Coast Guard Cyber Command
DHS NCCIC Liaison Officer
(202) 372-3113
Brett.R.Rouzer@uscg.mil

# Vision & Mission

## VISION

"A safe, secure and resilient cyber operating environment that allows for the execution of Coast Guard missions and maritime transportation interests of the United States."

## MISSION

The CGCYBERCOM mission is to identify, protect against, enhance resiliency in the face of, and counter electromagnetic threats to the Coast Guard and maritime interests of the United States, provide cyber capabilities that foster excellence in the execution of Coast Guard operations, support DHS cyber missions, and serve as the Service Component Command to U.S. Cyber Command.

***Computer Network Defense…Protecting MCIKR…Creating a Decision Advantage for the Service***


Homeland Security

# Mission Areas

Marine Safety

Ports, Waterways, and Coastal Security

**DHS Mission 4:** Cybersecurity

Provide a Secure Platform

Living Marine Resources

**DHS Mission 1:** Critical Infrastructure

**DHS Mission 2:** Secure Borders

**DHS Mission 4:** Cybersecurity

**DHS Mission 5:** Resiliency

Secure Ports and Waterways

Law Enforcement, Marine Safety

Counter Drug

Migrant Interdiction

**DHS Mission 1:** Enhancing Security

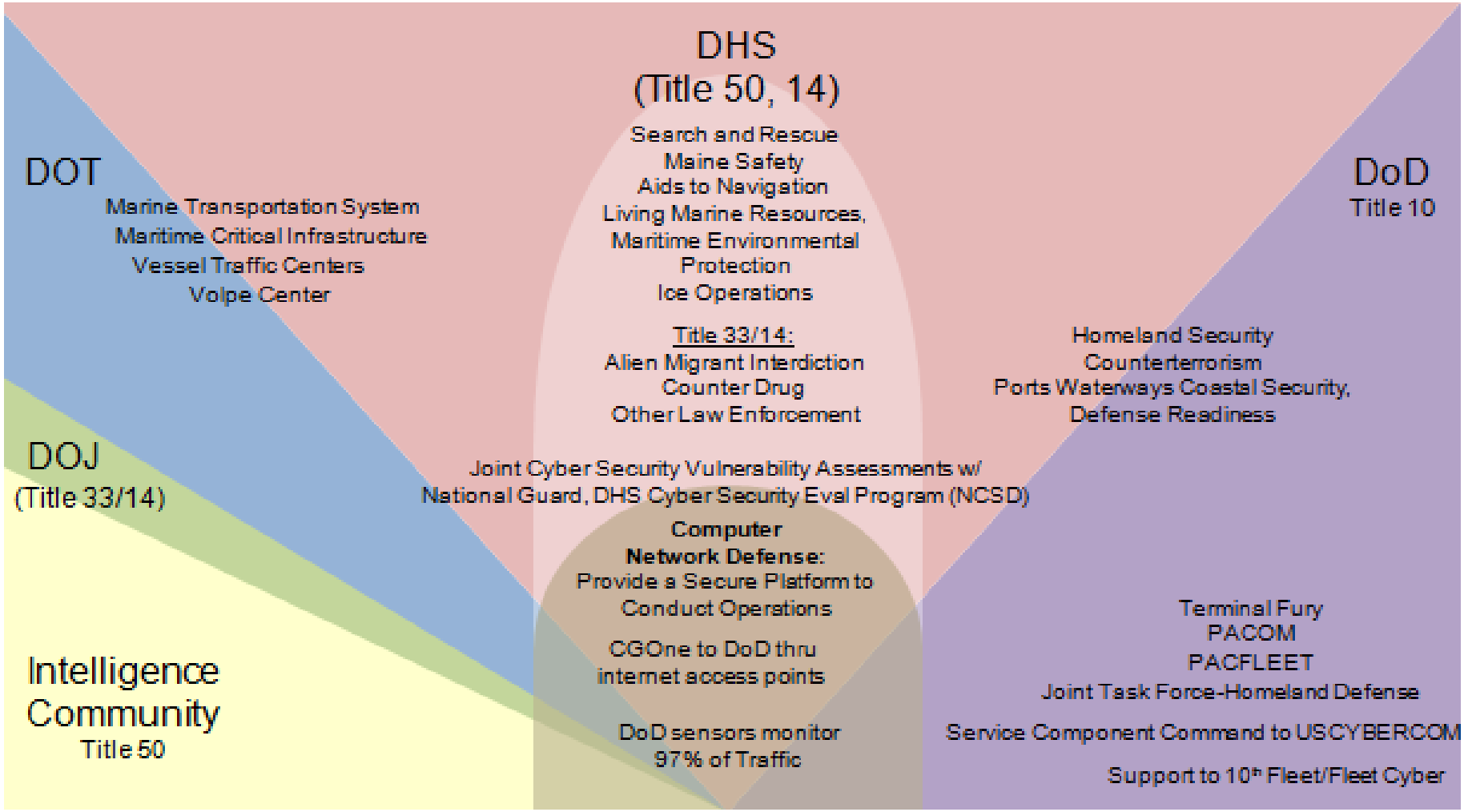
**DHS Mission 2:** Secure Borders

**DHS Mission 3:** Enforcing Immigration Laws

Provide Decision Advantage

Homeland Security

# CGCYBERCOM Nexus



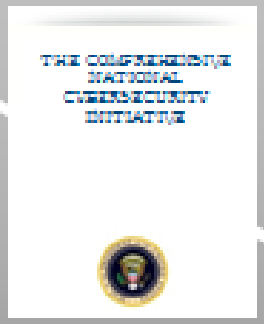

Homeland Security

# Strategic Mandates

- Federal Law
  - Maritime Transportation Security Act (MTSA) 2002
- Presidential Policy
  - National Security Strategy
  - National Infrastructure Protection Plan
    - Transportation Systems CIKR Sector-Specific Plan
  - National Strategy for Maritime Security
  - National Strategy to Secure Cyberspace
  - Critical Infrastructure Identification, Prioritization and Protection (HSPD-7)
  - National Preparedness (PPD-8)
- Departmental Guidance
  - DHS Strategy for Safeguarding and Securing Cyberspace

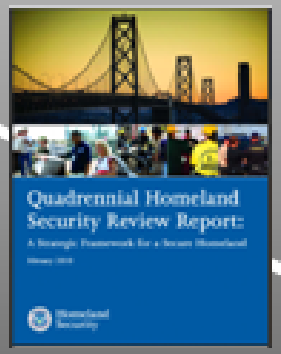
# Policy Linkage


National Security Strategy

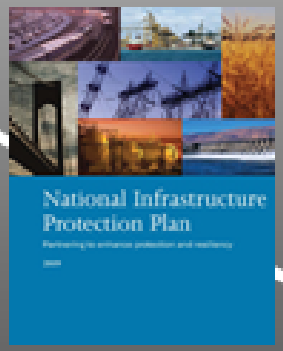


Roles, Responsibilities, Funding (CNCI)


Framework & Near Term Actions




Mission 4




National & CIKR Sector Level Plans

DHS Strategy for Safeguarding and Securing Cyberspace

2011

The CGCYBERCOM mission strategy for MCIKR Protection is being developed within the context of an existing strategy and policy framework that starts with the National Security Strategy.

Homeland Security

# Sector-Specific Plans (SSPs)


- Each SSA is responsible for writing a Sector-Specific Plan
- Latest Transportation Systems Sector-Specific Plan issued in 2010, with modal Annexes. Maritime Annex is not subordinate to the TS SSP, but is a component of.
- The Transportation Systems Sector has four primary goals: (TSSSP, 2010, p. 25-26)
  - Goal 1: Prevent and deter acts of terrorism using, or against the transportation system;
  - Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests;
  - Goal 3: Improve the effective us of resources for transportation security;
  - Goal 4: Improve sector situational awareness, understanding and collaboration.

# CGCYBER NIPP/CIKR Priorities

- Raise awareness and understanding of maritime cyber issues with port partners
- Develop proactive public-private partnerships utilizing existing Captain of the Port structures
- Form a comprehensive cyber risk picture
  - Cybersecurity Assessment and Risk Management Approach (CARMA)
  - Maritime Security Risk Analysis Model (MSRAM)
- Effectively share information
  - Cross-Sector Cyber Security Working Group (CSCSWG)
  - Industrial Control Systems Joint Working Group (ICSJWG)
  - Transportation Systems Sector Cyber Working Group (TSSCWG)
  - Cyber Unified Coordination Group (CYBER UCG)

# The Threat

NATURAL DISASTERS

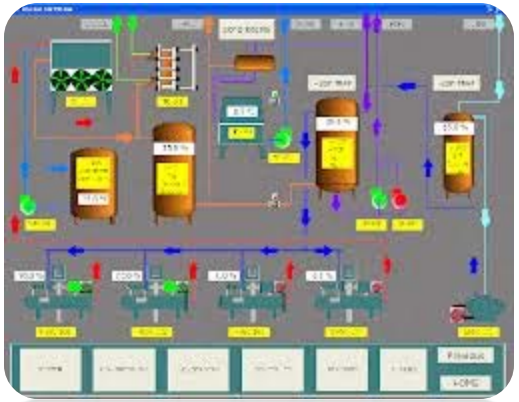
CRIMINALS

INSIDERS

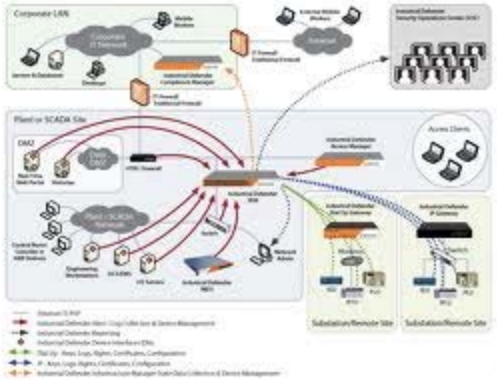
HACKTIVISTS

NATION STATES

# The Vulnerabilities



INDUSTRIAL CONTROL SYSTEMS




WIRELESS NETWORKS & SMARTPHONES

Homeland Security

# CGCYBER Products & Resources

- Weekly Cyber Feed…unclassified product geared toward raising awareness of key cyber vulnerabilities and threats. Shared with port partners directly via e-mail and posted on HOMEPORT
- Developing cyber MCIKR specific CYBER Community on HOMEPORT
- Quarterly cyber round table meeting
- Exercise support
  - On-site SME support
  - Exercise scenario development
- Working with CG-PSA-2 to develop cyber dimension for port vulnerability assessments
- Cyber awareness products

# Cyber Partnership with DHS

**National Cybersecurity and Communications Integration Center**

- DHS 24X7 cyber operations center
- National response center for coordination federal response to a cyber incident

**US-CERT**

- Coordinate cyber information sharing
- Vulnerability and risk assessments

**ICS-CERT**

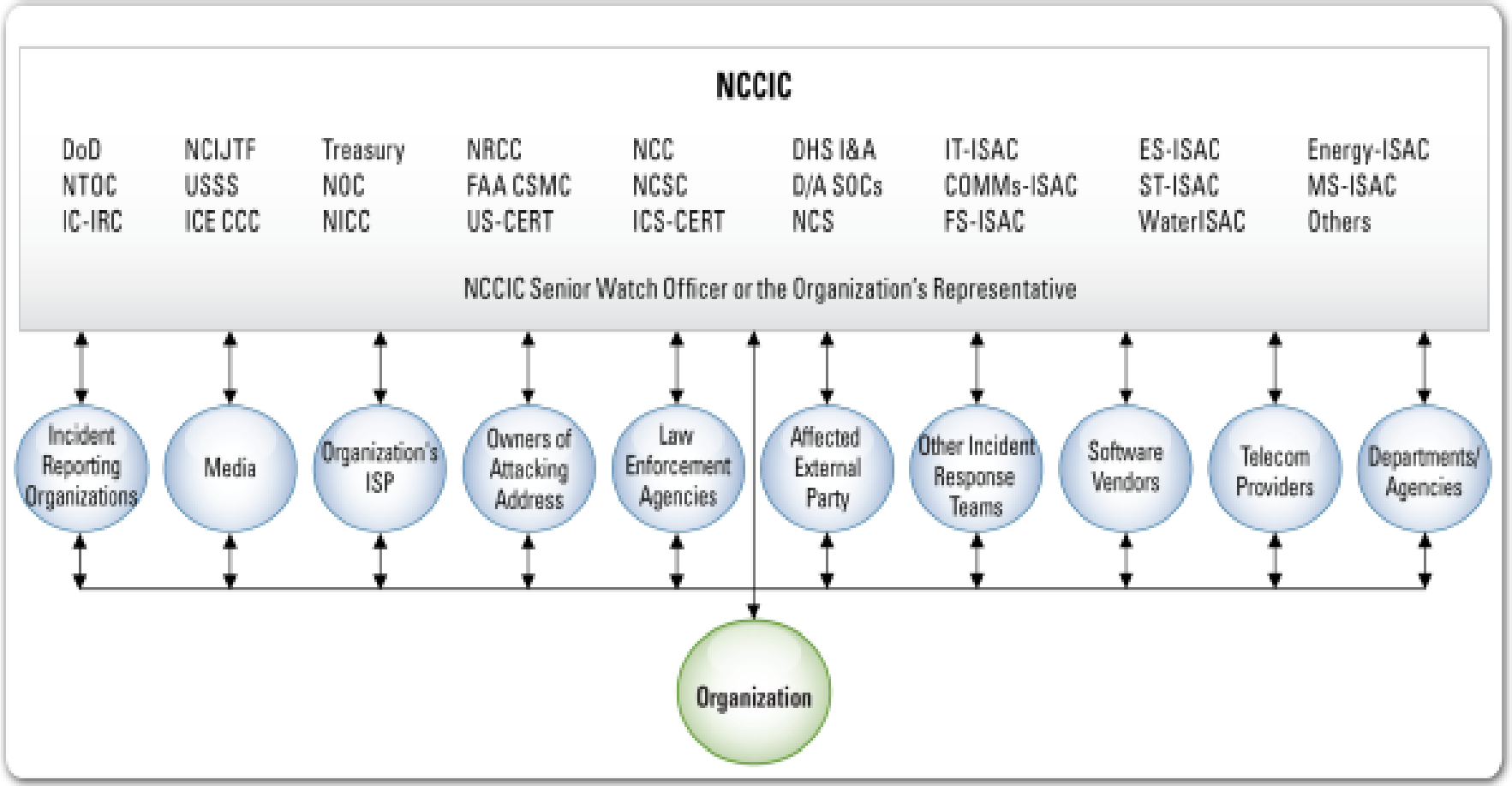
- Basic, intermediate and advanced cybersecurity and industrial control systems training
- On-site emergency response

**One DHS Cybersecurity Communications Strategy**

- One message from all DHS components

# Organizational Components And Operational Partners

## NCCIC Elements



# Cyber Unified Coordination Group (UCG)

An interagency and inter-organizational coordination body that incorporates public and private sector officials. It works during steady-state to ensure unity of NCCIC coordination and preparedness efforts and to facilitate the rapid response in case of a Significant Cyber Incident.

During a Significant Cyber Incident, the Assistant Secretary of CS&C coordinates with the Cyber UCG to develop an incident action plan, and activate the Cyber UCG Incident Management Team (IMT).

**Participation in the Cyber UCG:**

*Each Federal department and agency head; Chief Executive of a State, Locality, Tribe, or Territory; and designated private sector CIKR partners will be requested to designate at least two representatives*:

- a Cyber UCG **Senior Official who has policy and decision-making authority**; and
- a Cyber UCG **Staff member who works for the Senior Official's organization but has been designated to participate in NCCIC planning, preparedness and synchronization efforts.**

# CG-00 Direction…CGCYBERCOMs Value Proposition

## Mission Excellence and Building Capacity

- We have a unique role and authorities within DHS and they are not redundant
- Parity and partnerships with all cyber centers

## Enhance Response

- Improves the Service's ability to respond across the full spectrum of cyber threats with a more *capable* and *proficient* response option

## Prepare for the Future

- Professionalizing the CG's cyber community (training, tactics and decision advantage)…"high tides raise all boats."
- "Shrinking the box…" leverage cyber intelligence for operational advantage (similar to SIGINT)
- Tactical capability that is directly linked to S-1's strategic cyber direction

# Homeland Security

Brett Rouzer
Chief of MCIKR Protection
U.S. Coast Guard Cyber Command
DHS NCCIC Liaison Officer
(202) 372-3113
Brett.R.Rouzer@uscg.mil