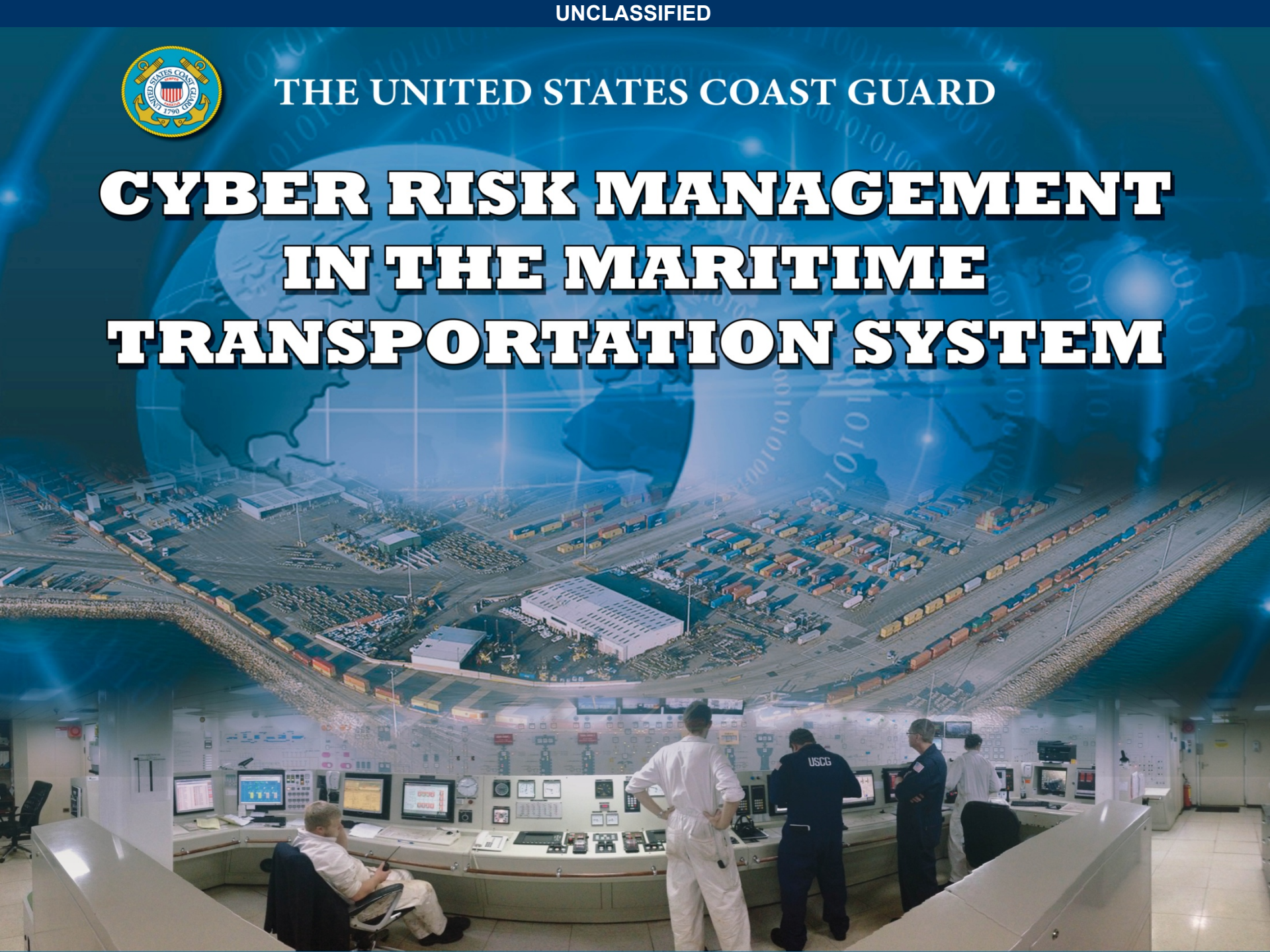
THE UNITED STATES COAST GUARD

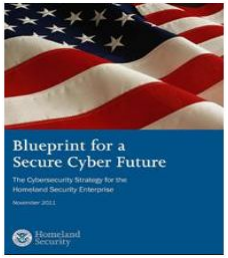
CYBER RISK MANAGEMENT IN THE MARITIME TRANSPORTATION SYSTEM

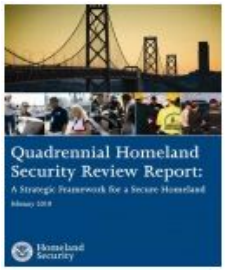


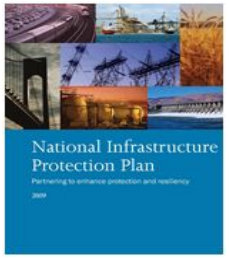
Policies, Directives and Mandates

Presidential / National Policy

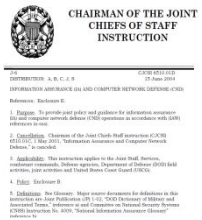
DHS Policies / Directives

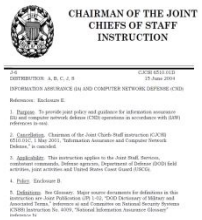






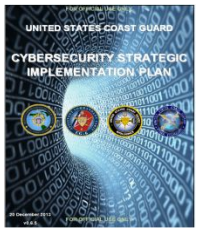
DOD Policies / Directives





CG Policies / Directives

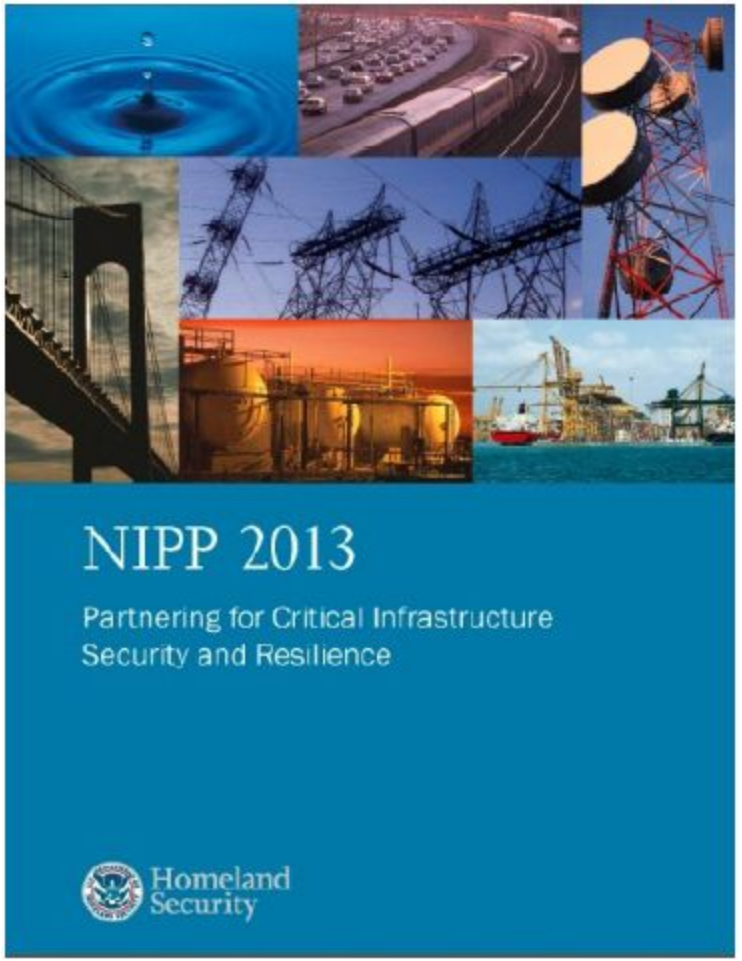
BEING DEVELOPED



Maritime Critical Infrastructure

The Coast Guard is the Sector Specific Agency (SSA) for the Maritime component of the Transportation Sector

- 1 of the 16 Critical Sectors
- Collaboration with our partners in TSA and DOT
- Protect maritime sector from all threats (physical, personnel, and ***cyber***)



EO 13636

- **EO 13636: Improving Critical Infrastructure Cybersecurity Directs the Executive Branch to:**
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

PPD-21

- **Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:**
- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan

PUBLIC MEETING ON 15 JAN

The Coast Guard is seeking public input on the following questions:

(1) What cyber-dependent systems, could lead to a TSI?

(2) What procedures or standards are used to id cybersecurity vulnerabilities?

(3) Are there existing cybersecurity assurance programs available?

(4) Cyber security training programs?

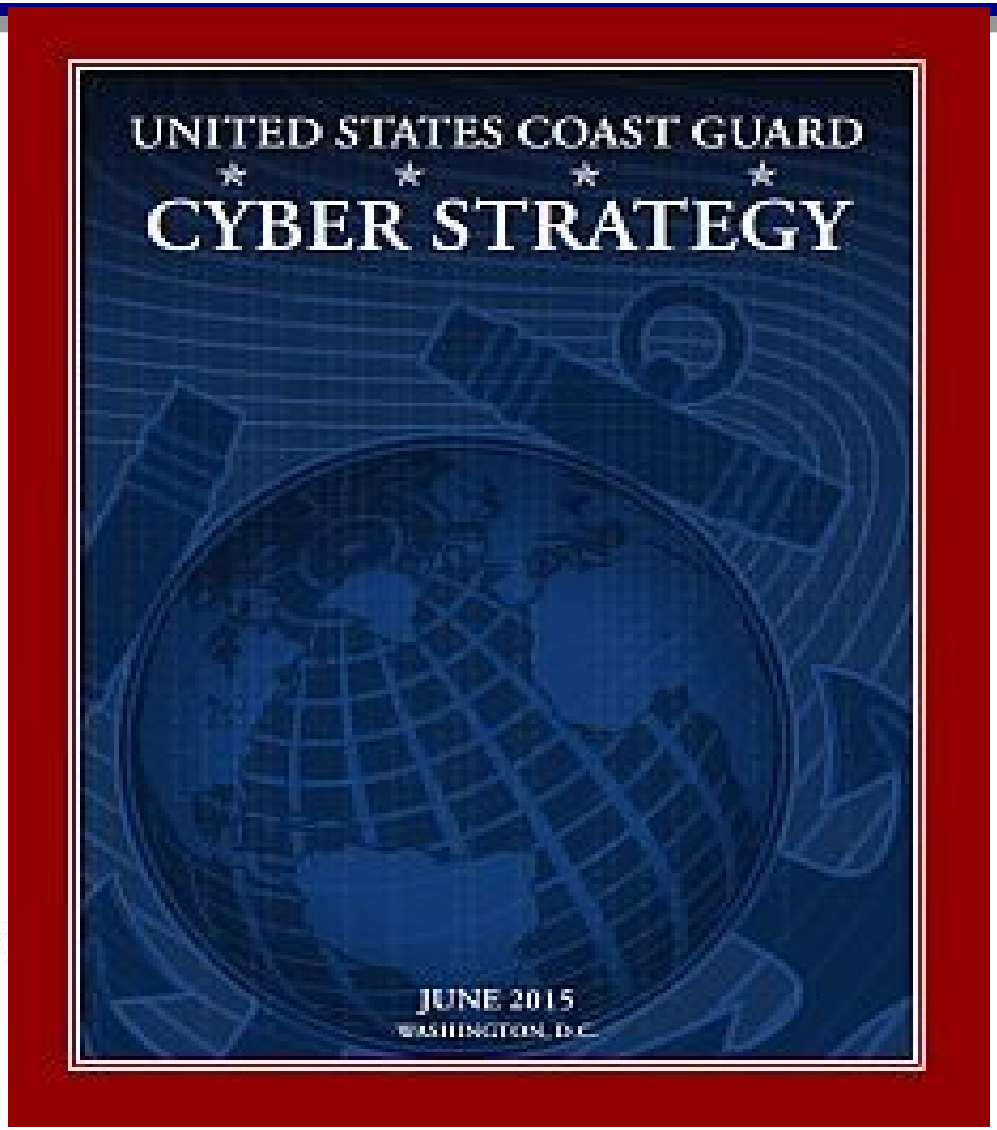
(5) When are manual backups or other non-technical approaches needed?

(6) How can Alternative Security Programs be used?

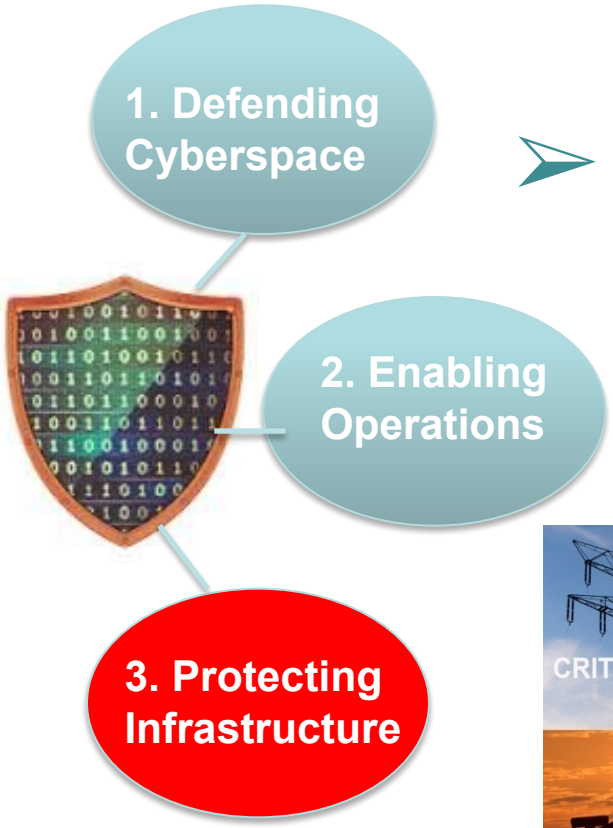
(7) How can Coast Guard verify technical or procedural standards?

(8) How do third parties (class, insurance, etc) play a role?

https://www.federalregister.gov/articles/2014/12/12/2014-29205/guidance-on-maritime-cybersecurity-standards


UNITED STATES COAST GUARD
CYBER STRATEGY
JUNE 2015
WASHINGTON, D.C.

3. Protecting Infrastructure



➢ Goal 1. Risk Assessment – Promote Cyber Risk Awareness and Management

What have we done since it was signed?

- MBLT Profile
- Review existing policy for cyber updates
  - IMO: Maritime Cyber Risk Management
- Standardize terms/definitions
- Evaluate guidance & tools for industry on risk reduction processes: FERC
- AMSC IT Subcommittees
- Cyber Event Reporting Process

Cyber Event Reporting

- NCCIC/NRC
- BOS Instruction

Available resources

- https://homeport.uscg.mil/
- http://www.nist.gov/cyberframework/
- https://www.us-cert.gov/

QUESTIONS?

Thank You for your time!

Further inquiries:
LCDR Josephine Long
Josephine.A.Long@uscg.mil
202-372-1109