AMSC Conference
Cyber Brief

- Cyber in the MTS
- Coast Guard Cyber Strategy
- Significant Accomplishments
- Reporting Requirements
- Ongoing Initiatives
- Best Practices

Cyber in the MTS

- Cyber threats are a growing portion of the total risk exposure faced by the MTS
    - ➢ Gulf Coast area refinery (thumb drive)
    - ➢ Saudi-Aramco (destroyed ~ 30,000 computers)
    - ➢ Container terminal in Hampton Roads (GPS)
- As a community, need to recognize and address cyber affects holistically and not limit it to an "IT problem".

Coast Guard Cyber Strategy

- USCG Cyber Strategy has three parts:
  - Computer Network Defense
  - Maritime Superiority
  - MTS Cyber Security

Significant accomplishments

- General cyber guidance to Coast Guard field units.
- Alerts, advisories, best practices on Homeport
- Cooperation w/interagency to provide tools to industry (C2M2, CARMA)
- Increased awareness and conversation with partners at local level nation-wide.

Guidance to Field

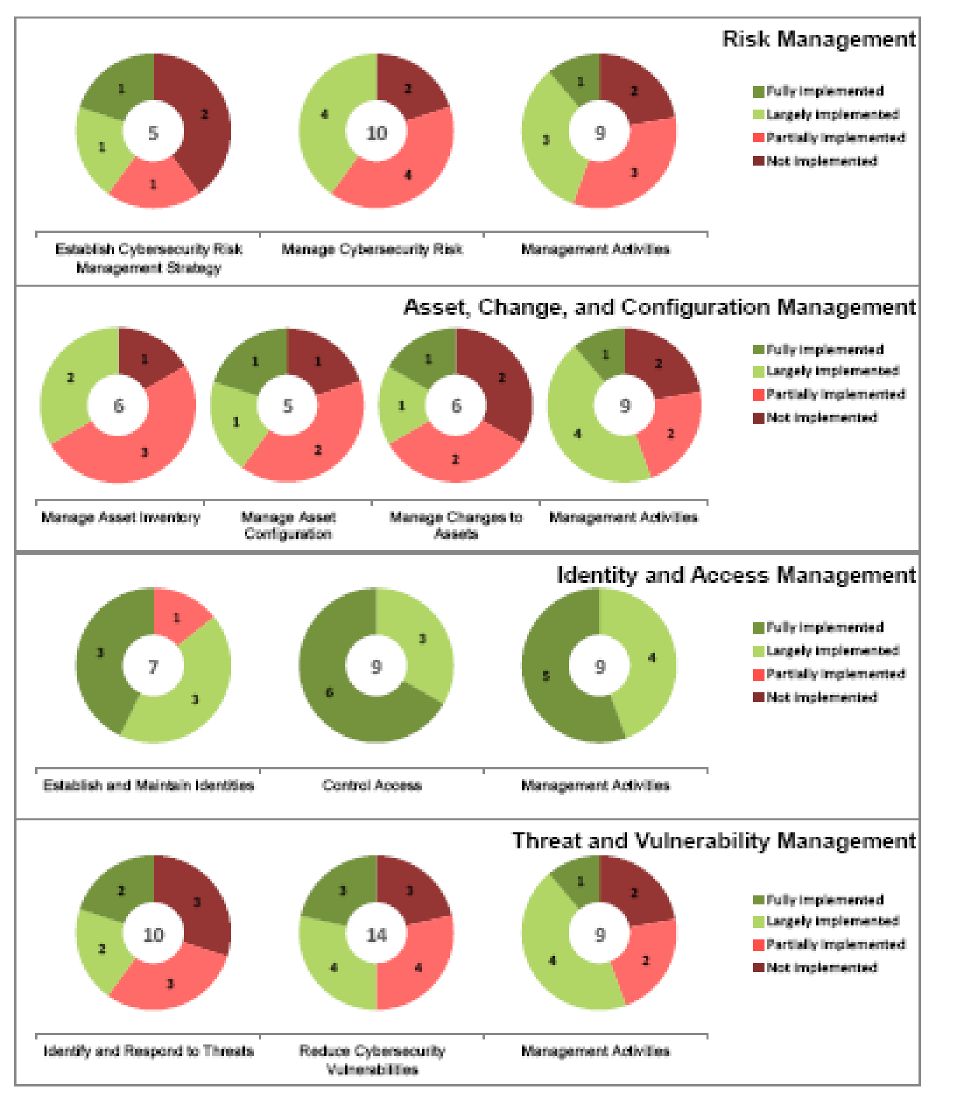
- NVIC 9-02, change 4 (June 2013).
- ALCOAST 323/13 (August 2013)
- ALCOAST 122/14 (March 2014)

Cyber Capability Maturity Model

Department of Energy Tool originally developed pre-NIST

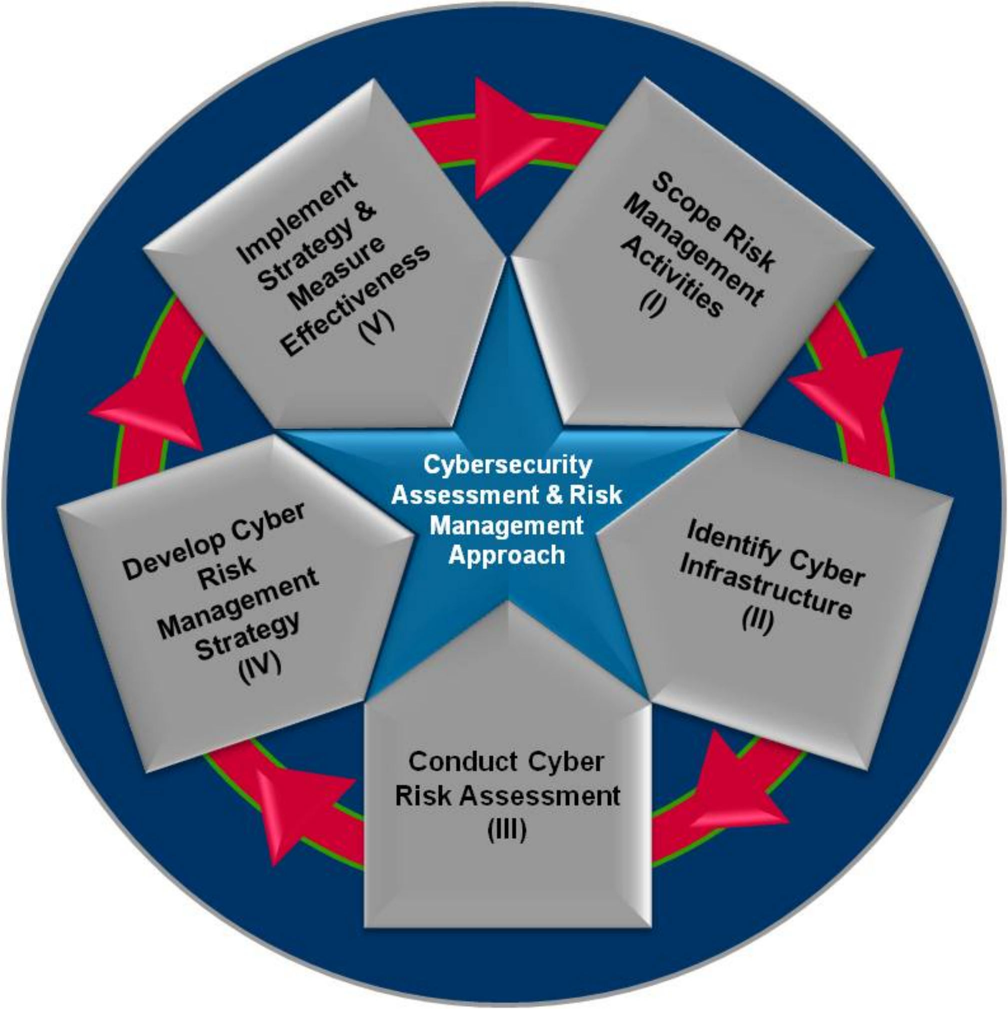
Worked with DHS and DOE to develop a maritime version

Beta test successfully completed with a maritime company



Cyber Security Assessment and Risk Management Approach (CARMA)

- System used to evaluate national level cyber CI risks to meet Executive Order requirements
- Worked with DHS to develop a port-level version
- Beta testing will be conducted at a port later this year.



Cybersecurity Assessment & Risk Management Approach
Scope Risk Management Activities (I)
Identify Cyber Infrastructure (II)
Conduct Cyber Risk Assessment (III)
Develop Cyber Risk Management Strategy (IV)
Implement Strategy & Measure Effectiveness (V)

Cyber Suspicious Activity/Incident Reporting

- Report Cyber suspicious activity and security incidents (breaches of security) to the NRC at **800-424-8802**.

- Reporting is **REQUIRED** for incidents meeting the definition in **33 CFR 101.305**

Ongoing Initiatives

- Continue development of the CG Cyber Strategy
- Continue to evaluate and distribute voluntary risk assessment tools to industry
- Incorporate Cyber Security in pending Facility Security Officer Course regulation
- Incorporate cyber to port security assessments
- Improve NVIC 9-02, ch-4 guidance to AMSCs

What your Organization Should Do

- Establish a healthy cybersecurity culture
- Insider threat- report high-risk behavior
- Exercise- practice makes perfect
- Scrutinize acquistions/contracting practices
- Emphasize that cybersecurity is not just a job for the IT Department

What Should You Do Individually?

- Maintain updated software and operating systems
- Use difficult passwords
- Encrypt files and enable certificates
- Secure PII/mobile devices
- Recognize phishing and other social engineering

Questions