Coast Guard Cyber Command

Driving Mission Execution

CAPT John Felker
Deputy Commander, CGCYBERCOM

June 2011
Cyber Definition

- New Domain (ex. Air, Sea, Space)
- Electromagnetic Spectrum
- Threats/Vulnerabilities
- Legal/Ethical/Technical Issues
“Develop capabilities to resist and respond to cyber threats. In addition to our own forces, the vast port and maritime transportation systems we protect are vulnerable to cyber attack. Work with our partners to develop resiliency to cyber threats.”
Mission Areas

MISSION 1.4: CIKR
- Homeland Security/Counter Terrorism
- Maritime CIKR
MISSION 2: Securing Borders
MISSION 3: Enforcing Immigration Laws
MISSION 4: Cybersecurity
MISSION 1.4: CIKR
MISSION 5: Resiliency

Provide a Secure Platform
Secure Ports and Waterways
Provide Decision Advantage
Cyber Gaps - Secure Ports and Waterways

MTS Mission
- Execution
- Resources/guidance

Vulnerabilities
- Proprietary systems
- Ease of access vs. security

Coordination
- DCO / Prevention community
- DHS
- Industry
MTS Cyber Systems with Vulnerabilities

- Control Systems - SCADA
- Aids to Navigation
- Communications
- Vessel Traffic Services

Coast Guard has responsibility.
- 33 CFR 103
Threats to MTS Cyber Systems

- Nation-states
- Criminals
- Hacktivists
- Natural disasters
- Internal users – self-inflicted gun shot wounds

Coast Guard has responsibility.
- 33 CFR 103
Maritime Transportation System (MTS) Scenario

$$$

$$$

$$$
Response and Recovery Coordination

Multiple agencies could be called upon for support...

- DHS NCSD – NCCIC (US-CERT & ICS-CERT)
- National Guard Bureau
- FBI
- USCYBERCOM
- Others
Strategic Information Sharing

- Cross-Sector Cyber Security Working Group (CSCSWG)
- Industrial Control Systems Joint Working Group (ICSJWG)
- Transportation Systems Sector Cyber Working Group (TSS CWG)
- Ports, waterways, and shores are lined with CIKR facilities (nuclear power plants, oil refineries, pipelines, chemical plants, bridges, etc.)
  - ALL linked to cyber systems or networks and rely on industrial control systems

DHS/USCG Effort –
- MTS partners better understand issues
- Develop consistent approach
Tactical Information Sharing

- COTP threat notification required
- Owner/Operators security or TSIs reporting

**END STATE DESIRED** –
  - Process & culture of open/frank information sharing
Outreach Support

Support port partners:

• Review of plans (threats, vulnerabilities and consequences)

• Joint cyber workshops with COTP

• Information sharing

...end goal is effective preparation, response and recovery

...RESILIENCE
Where We Want to Focus

- **External Factors**
  - Cyber Attack
  - Natural disaster
  - Etc.

- **Inside Your Network**
  - System degradation
  - Loss of positive control
  - Etc.

- **Operations Impact**
  - Physical outcome
  - Loss of capability
  - Etc.
QUESTIONS?
• CAPT John Felker, Deputy Commander  
  – John.M.Felker@uscg.mil
• CDR Cliff Neve, Chief of Network Defense, Intelligence, & Operations  
  – Jack.C.Neve@uscg.mil
• LT Lars McCarter, Network Defense  
  – Harold.L.Mccarter@uscg.mil
• LT Will Towers, Operations  
  – William.A.Towers@uscg.mil
• Mr. Scott Dickerson, CG-5322-3 Liaison & Operations Support  
  – Scott.A.Dickerson@uscg.mil