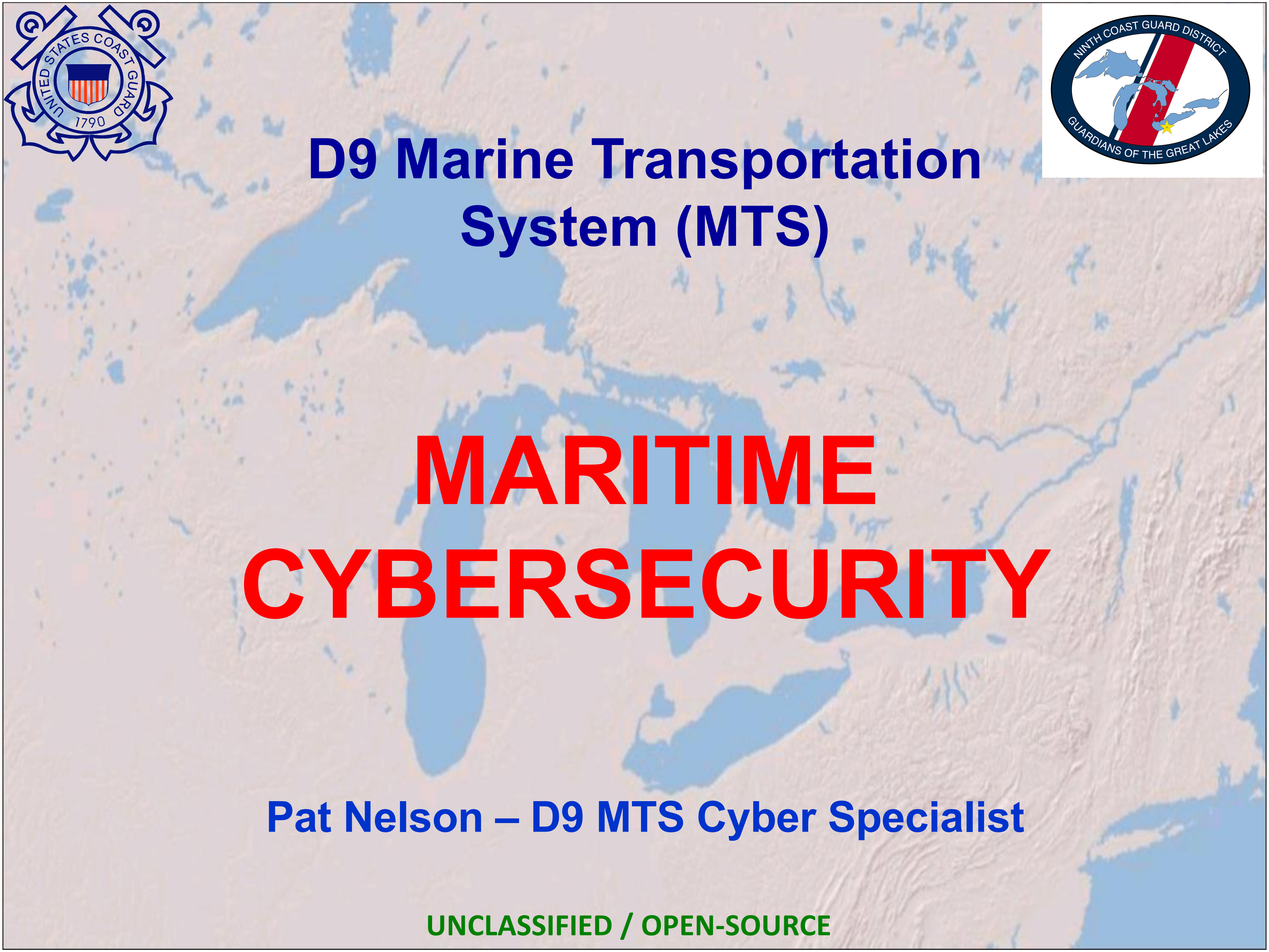


D9 Marine Transportation System (MTS)

MARITIME CYBERSECURITY

Pat Nelson – D9 MTS Cyber Specialist

UNCLASSIFIED / OPEN-SOURCE

MTS CYBER

WHY MTS CYBER:

"Cyber attacks against the United States (U.S.) are one of the most significant threats to our economic and military power since World War II. The events of the last five years, including the exploitation of U.S. Coast Guard networks and information, attacks on maritime critical infrastructure, and adversarial efforts to undermine our democratic processes, reinforce that cyberspace is a contested domain."

–CG 2021 Cyber Strategic Outlook

"Escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security… U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win, against nation-states intent on disrupting or destroying our critical infrastructure. Bold action is needed to prevent the dire consequences of a catastrophic cyber attack."

-President's National Infrastructure Advisory Council report Dec 2019

UNCLASSIFIED / OPEN-SOURCE

MTS CYBER

NATIONAL LEVEL THREATS BECOME LOCAL:

- **Iranian Centrifuges (2010):** Machines self-destructing
- **Port of Antwerp (2011):** Drug cartel hijacking container management
- **Ukraine Power Grid Attacked (2015 & 2016):** Infrastructure Threat
- **Maersk Line Disrupted (2017):** Intentional destruction, massive maritime impact
- **Port of Kennewick (2020):** Ransomware, e-mail and other systems
- **SolarWinds Orion Breached (2020):** Supply chain, ~18k systems
- **Microsoft Exchange Server Breached (2021):** 30k+ organizations
- **Florida Water Treatment Attacked (2021):** Attempt to poison water
- **Purported Iran Cyber Files (2021):** Fuel pumps, cargo ships (satellite comms, ballast systems)
- **Port of Houston (2021):** Attributed to “nation-state actor”, successfully defended

MTS CYBER

RECENT EVENTS RELEVANT TO OPERATIONAL TECHNOLOGY

- **CISA Shields-Up among other recommendations, advises: "Plan for the Worst: While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario."**

- **FBI/CISA/NSA/DOE alert AA22-103 of April 2022: "certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices."**

UNCLASSIFIED / OPEN-SOURCE

MTS CYBER

RECENT EVENTS RELEVANT TO OPERATIONAL TECHNOLOGY

- **FBI/CISA/DOE alert AA22-083A March 2022 indicated threat actors have "conducted a multi-stage campaign in which they gained remote access to U.S. and international Energy Sector networks" and have "gained access to and leveraged … malware to manipulate a foreign oil refinery's ICS [Industrial Control System] controllers."**

- **FBI/CISA alert AA22-076A of March 2022 regarding satellite communications indicated that the FBI and CISA are aware of possible threats of intrusion into satellite communication networks that "could create risk in SATCOM network providers' customer environments."**

MTS CYBER

RESOURCE UPDATE

- **Coast Guard Marine Safety Information Bulletin 02-22 of 11 April 2022, includes: "While breaches of security and suspicious activity are required to be reported to the NRC, the Coast Guard's Cyber Command is available to provide technical support to help MTS stakeholders prepare for or respond to a cyber-incident. Their 24x7 watch can be reached at: 202-372-2904 or CGCYBER-SMB-NOSC-BWC@uscg.mil ."**

- **Coast Guard Cyber Protection Teams available for voluntary cyber risks assessments, free of charge**

- **Hiring on of Sector MTS-Cyber Specialists**

UNCLASSIFIED / OPEN-SOURCE

MTS CYBER

OK, WHAT DO WE DO?

Identify, Protect, Detect, Respond, Recover

- *National Institute of Standard and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity*

RISK-BASED COORDINATION, PLANNING/EXERCISES

- 46 USC 70103(b)(2)(H): The FMSC shall submit an Area Maritime Transportation Security Plan that includes “a plan for detecting, responding to, and recovering from cybersecurity risks that may cause transportation security incidents”

MARITIME TRANSPORTATION SECURITY ACT (MTSA) / INTERNATIONAL MARITIME ORGANIZATION (IMO)

- Apply Prevention and Response Frameworks
- MTSA/IMO cyber requirements for facilities and vessels

MTS CYBER

IDENTIFY:

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

LINES OF EFFORT

- **Awareness of ever evolving threats to the MTS**
  - Characterize threats through adversary intent and capability
- **Coordinate, develop, exercise**
  - AGLPA/AMSC/HSC/Area Cmte
- **Risk Assessment**
  - Coast Guard Cyber Protection Teams (CPT)
  - Cybersecurity and Infrastructure Security Agency (CISA) resources
  - MTSA – FSA/VSA – 33 CFR
    - Facilities starting 01 October 2021
    - Vessels starting 31 December 2021 (or earlier)
- **Develop Expertise**

MTS CYBER

PROTECT:

Develop and implement appropriate safeguards to ensure delivery of critical services.

LINES OF EFFORT

- **Coordination**
  - Coordinate with partners to support maritime cybersecurity capacity building, training, and port security risk management
- **Risk Reduction**
  - Port Security Grant Program
- **Implement a risk based regulatory, compliance and assessment regime**
  - MTSA/IMO – FSP/VSP
- **Data security and maintenance**
  - Culture of cyber hygiene

MTS CYBER

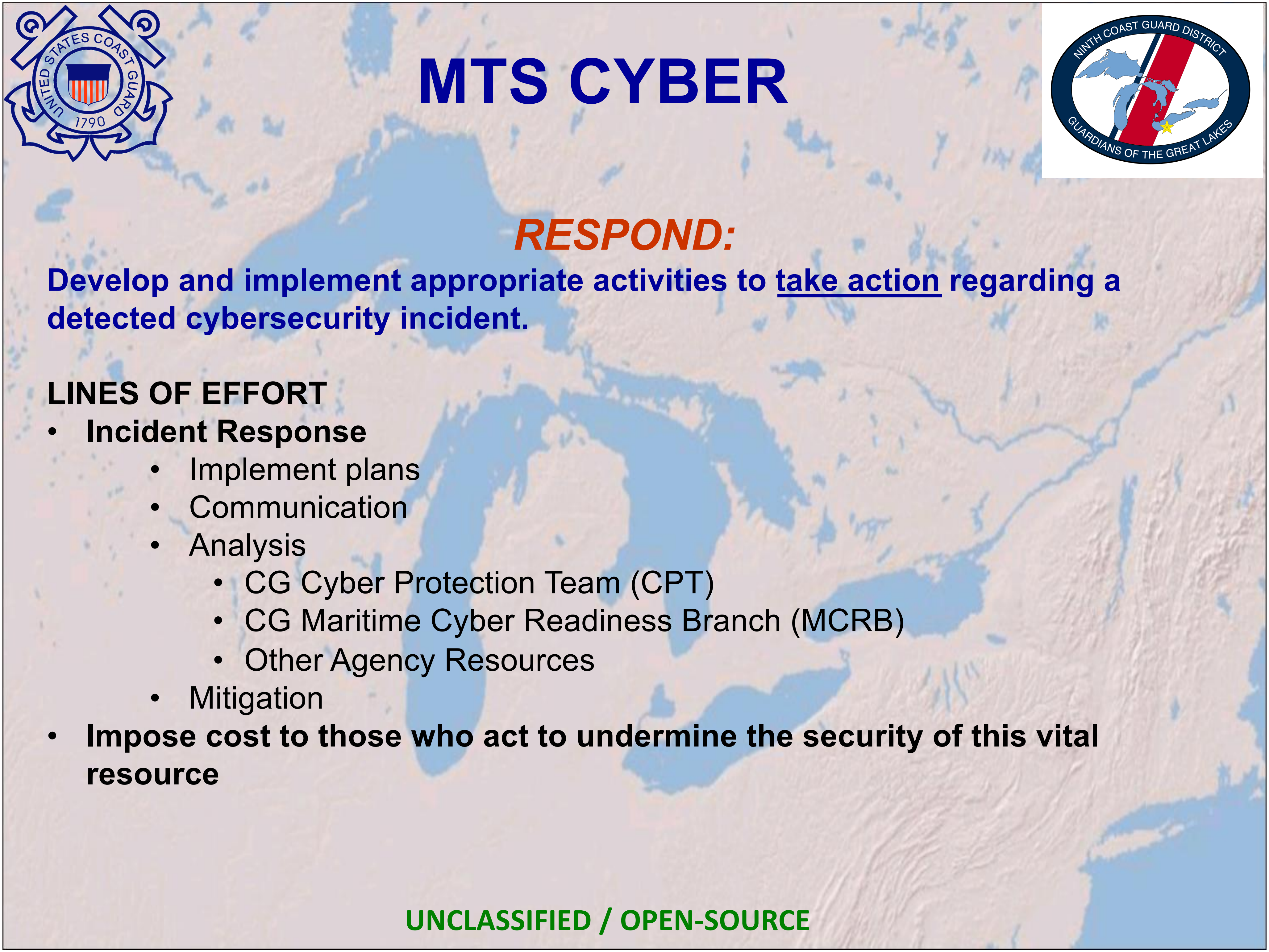
DETECT:

Develop and implement appropriate activities to identify the <u>occurrence of a cybersecurity event</u>.

LINES OF EFFORT

- **Promote information sharing**
    - Incident Response Plans
        - Anomalies and events
        - Detection processes
- **Refine cybersecurity incident reporting requirements**
    - CG-5P Policy Letter 08-16
- **Promulgate threat advisories to the maritime community**
    - CISA Alerts

MTS CYBER



RESPOND:

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

LINES OF EFFORT

- **Incident Response**
  - Implement plans
  - Communication
  - Analysis
    - CG Cyber Protection Team (CPT)
    - CG Maritime Cyber Readiness Branch (MCRB)
    - Other Agency Resources
  - Mitigation
- **Impose cost to those who act to undermine the security of this vital resource**

MTS CYBER

RECOVER:

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

LINES OF EFFORT

- **Recovery Planning -** Recovery processes and procedures are executed and maintained
  - **Recovery Playbook**
- **Improvements -** Incorporating lessons learned
- **Communication -** Restoration activities are coordinated with internal and external parties

- **National Institute of Standard and Technology (NIST)**
  - Framework for Improving Critical Infrastructure Cybersecurity
  - Special Publication 800-184 Guide for Cybersecurity Event Recovery

MTS CYBER

- Recently published CG Cyber Strategic Outlook available at: https://www.uscg.mil/Leadership/Senior-Leadership/Resource-Library/
- 5P Cyber Incident Reporting Requirements: https://www.dco.uscg.mil/Portals/10/Cyber/Cyber-Readiness/CG-5P%20Policy%20Letter%2008-16%20-%20Reporting%20Suspicious%20Activity%20and%20BoS.pdf?ver=2020-05-26-173911-100&timestamp=1590758815625
- USCG Commercial Vessel Compliance Cyber Work Instruction CVC-WI-027(2): https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Commercial-Vessel-Compliance/CVCmms/
- CG-FAC cyber page: https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/
- CISA Cyber Essentials Starter Kit: https://www.cisa.gov/cyber-essentials
- CISA Alerts: https://us-cert.cisa.gov/ncas/alerts
- CISA Cyber Resilience Review (CRR) available at: https://us-cert.cisa.gov/resources/assessments
- NIST framework available at: https://www.nist.gov/cyberframework
- NIST guide for cybersecurity event recovery: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

UNCLASSIFIED / OPEN-SOURCE

UNITED STATES COAST GUARD 1790

MTS CYBER

NINTH COAST GUARD DISTRICT
GUARDIANS OF THE GREAT LAKES

Questions?

UNCLASSIFIED / OPEN-SOURCE