U.S. COAST GUARD
CYBER PROTECTION TEAM (CPT)

Our Team

Based in Washington, D.C., CPTs are the Coast Guard's deployable units responsible for offering cybersecurity capabilities to partners in the Marine Transportation System (MTS).

The USCG possesses two CPTs with three deployable elements each, as well as intel and mission support. CPTs consist of Active Duty and Civilian Coast Guard cybersecurity professionals trained and certified in delivering three core capabilities: **Assess, Hunt, and Incident Response.**

Assess

Penetration Testing:
Determine susceptibility to a real world incident by identifying weaknesses in security through internal or remote emulation of cyber threat actors.

Configuration Review:
Analyze operating system and database settings and configurations compared to industry standards, guidelines, and best practices.

Hunt

Threat Hunting:
Missions driven by the latest vulnerability reporting to illuminate known or unknown adversaries on a network and determine the scope and impact of a potential compromise.

Incident Response

Integrate forensic analysis, cyber threat intelligence, and further government support including FBI, CISA, and other agencies into response actions. Utilize CPT cybersecurity experts to advise mitigation and remediation steps to recover from the incident.

Role in the Marine Transportation System

A critical component of the national supply chain, the MTS is increasingly reliant on computer networks and systems for efficiency and safety.

The CPT's mission is to enhance the resiliency of MTS Critical Infrastructure against cyber disruption through consistent proactive missions with public and private industry organizations.

CPTs deploy to conduct missions in support of MTS partners of varied size, functions, and expertise. To date, USCG CPT has supported 30+ MTS partners.

Mission Timeline

Planning

- After requesting a mission, a CPT will work with you to determine the capabilities, scope, parameters of the mission and logistics that fit organization and CPT requirements.

Mission Execution

- CPT missions are typically 1-2 weeks onsite or in a hybrid remote/onsite format depending on selected capabilities and scope.

Post-Execution

- Out-Brief: CPT will provide initial findings to trusted points of contact at end of the mission.
- A full technical report will be provided 45 days after the end of the mission.

How to Request CPT Support

To discuss capability details and what a CPT can do for your organization, contact us at MaritimeCyber@uscg.mil for a tailored introduction. Request are prioritized based on the time, nature, and criticality. Incident Response support should be communicated via the National Response Center (800-424-8802). Initial steps to request CPT Assess and Hunt support are below:

1. Contact your local USCG Sector or MaritimeCyber@uscg.mil and let them know you are interested in a CPT visit.

2. The Coast Guard will need a signed Request for Technical Assistance (RTA) to schedule mission dates.

For more detail visit us at https://dco.uscg.mil/Our-Organization/CGCYBER/Maritime-Cyber-Readiness-Branch/