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

Our Team

Based in Washington, D.C. CPT is the Coast Guard's deployable unit responsible for offering cybersecurity capabilities to the Marine Transportation System (MTS).

CPT consists of three teams of active duty Coast Guard cybersecurity professionals who are trained and certified in delivering the four core CPT capabilities: **Assess, Hunt, Clear and Harden**.

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 engagements with public and private industry organizations.

The CPT stands ready for worldwide deployment to conduct operations.

Engagement Timeline

Planning

- After requesting an engagement, the CPT will work with you to determine the capabilities, scope, parameters of engagement and logistics that fit organization and CPT requirements.
- Establish trusted points of contact and schedule of key milestones and deliverables leading up to engagement.

Engagement Execution

- CPT engagements 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 engagement.
- A full report will be provided 10 days after end of engagement.

CPT Core Capabilities

Assess

Penetration Testing:
Determine susceptibility to a real world incident by identifying weaknesses in security through internal or remote emulation of the tactics, techniques and procedures 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:
Information-driven operations to illuminate known or unknown adversaries on a network and determine the scope and purpose of a potential compromise.

Clear

Incident Response:
Assist stakeholders with targeting, containing and clearing malicious activity from cyber systems. Identify indicators of compromise to enhance security posture.

Harden

Remediation of Vulnerabilities:
Recommend best practices for securing systems against specific findings of **Assess** or **Clear** engagements.

Get Started

To discuss capability details and what CPT can do for your organization, contact us at MaritimeCyber@uscg.mil. Capabilities delivery queues will be continually prioritized based on the time, nature and criticality of the request. The prioritization process prevents a disproportionate amount of resources for any specific stakeholder(s) and ensures that any data associated or lessons learned from the capability provided is representative of the sector and nation.