U.S. COAST GUARD
MARITIME CYBER READINESS BRANCH

Our Team

The Maritime Cyber Readiness Branch (MCRB) is a cross-functional team of operations and cybersecurity professionals that support maritime cyber incident response activities and facilitate cyber threat information sharing.

To fulfill this unique integration, MCRB maintains a 24/7 watch that investigates and assesses all cyber incidents in the Marine Transportation System (MTS) that are reported to the Coast Guard (USCG).

MCRB bridges local, regional, and national efforts by advising the Captain of the Port (COTP) and senior leadership. By mitigating potential critical information gaps, MCRB strengthens risk management and the USCG's capability to protect critical infrastructure, systems, and operations, ultimately improving maritime security and resilience.

Role in the Marine Transportation System

MCRB proactively works with MTS stakeholders, private and public industry, and USCG units to help others understand the critical role of cybersecurity in their work. Nationwide collaboration and dissemination of the latest threat information allows partners to protect and defend against relevant threats targeting the marine environment.

Mission Set

Cyber Incident Response

- Provide direct assistance in incident investigations, including conducting interviews with impacted entities to remediate incidents.
- Act as subject matter expert advisors to the COTP and investigators to evaluate risks for decision-making.
- Facilitate the solicitation and coordination of Cyber Protection Team (CPT) services to mitigate the impact of the incident.

Outreach and Engagements

- Publish Maritime Cyber Alerts and Bulletins to facilitate timely cyber threat information sharing.
- Support and participate in cyber tabletop exercises, enhancing stakeholder cyber literacy and incident response training.
- Share the latest insights on emerging cyber threats and best practices with industry leaders through speaking engagements.
- Advise USCG Prevention community & operational commanders on the technical implementation of cyber regulations, policy, and direction.

Operational Planning:

- Create a unified response on cyber defense strategy with interagency partners such as the Department of Defense, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, and other stakeholders.
- Offer CPT 101 briefs on cyber services, capabilities, and trends to align mission objectives with partner needs.

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. Requests are prioritized based on time, nature, and criticality. Incident Response support should be communicated via the National Response Center (800-424-8802). Initial steps to request CPT Assessment 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 to schedule mission dates.

For more details, visit us at https://www.uscg.mil/MaritimeCyber/