CYBERSECURITY AWARENESS BULLETIN

WHEN AND HOW TO REPORT CYBERSECURITY INCIDENTS

Serial:	CI-AWA-2020-170-01
Date:	18 JUNE 2020

Scope

This bulletin provides guidance for the reporting criteria of cybersecurity incidents as well as information on how to report incidents depending on whether they involve Coast Guard Auxiliary National information technology systems or U.S. Coast Guard assets.

Summary

Cybersecurity incidents are more and more prevalent in our digital lives. An important way to protect yourself and others from cybersecurity incidents is to watch for them and report any that you find. Early detection can assist faster mitigation and enhance future prevention.

A cybersecurity incident is the violation of an explicit or implied security policy. Types of activity that are commonly considered as being in violation of a typical security policy include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data, including PII related incidents
- Unwanted disruption or denial of service
- Unauthorized use of a system for processing or storing data
- Unauthorized destruction or modification of data
- Unauthorized changes to system hardware, firmware, or software characteristics
- Phishing attempts to solicit personal information or execute malicious software from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been
- Malware incidents designed to damage or perform other unwanted actions on a computer system

Details

Any incident that meets the criteria above should be reported to an incident response center. As Auxiliarists, there are certain scenarios that direct what response organization should be notified.

Personal Accounts, Systems, and Data

Cybersecurity incidents that only involve personally owned or managed IT assets should be reported to appropriate telecommunications providers (i.e. your internet service provider) or account providers (such as Google, Microsoft, Yahoo, etc…). Incidents of a criminal nature should be reported to your local or state law enforcement agency's cybercrime organizations. Additionally, they may be reported to the US-CERT at https://us-cert.cisa.gov/forms/report or to the FBI Internet Crime Complaint Center at https://www.ic3.gov.

Coast Guard Auxiliary Accounts, Systems, and Data

Cybersecurity incidents that involve CGAUX National IT Systems and Accounts shall be reported to the Computer Software & Systems Directorate' s Cybersecurity Division (CI) by visiting http://wow.uscgaux.info/content.php?unit=C-DEPT&category=cybersecurity and selecting "Submit Incident Report". The Cybersecurity Division will coordinate the response with any necessary partner organizations. Those incidents or suspected incidents should be reported immediately upon discovery (do not delay to investigate yourself). Incidents where there is a possible compromise of Auxiliary personally identifiable information or operational information should also be reported to the CI Division immediately. Incidents that do not involve National Auxiliary IT systems data or accounts, but do involve other forms of CGAUX data may also be reported to CI.

U.S. Coast Guard Accounts, Systems, and Data

Cybersecurity incidents that involve USCG accounts, systems or data must be reported to Coast Guard Cyber Command immediately using appropriate channels. The CI Division can be reached to assist with notifications, if necessary.