U.S. Coast Guard Auxiliary Cybersecurity Awareness

October 2025

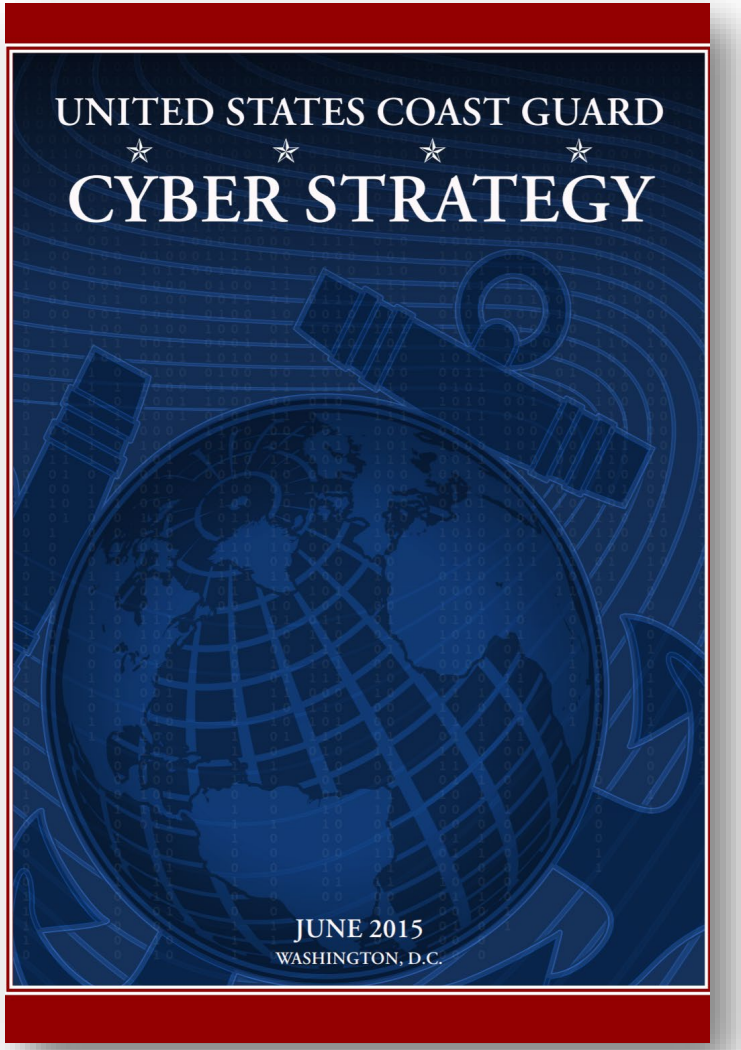
U.S Coast Guard Auxiliary

Introduction

The purpose of this workshop is to:

- Explain the importance of cybersecurity for each member
- Describe industry best practice in cybersecurity hygiene
- Discuss special considerations for members with access to USCG systems and data
- Outline reporting mechanism for cybersecurity incidents

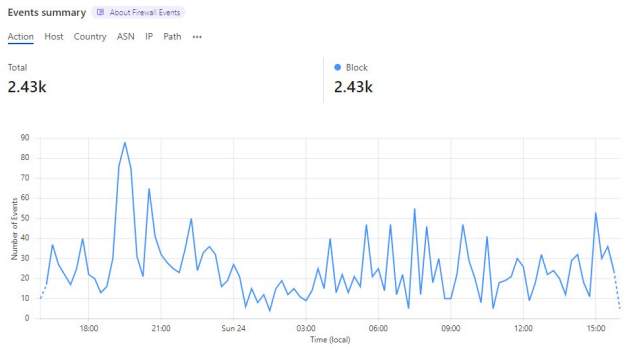
Everyone Has Responsibility



The Coast Guard must promote a culture that recognizes the importance of cyberspace operations, which has become just as important as operations in physical domains. operational commands at all levels must develop objectives and expectations for cyberspace operations within their areas of responsibility, and ensure that the cyber component is considered in all mission planning and execution. additionally, ***every Coast Guardsman—enlisted, officer, civilian, reservist, or auxiliarist—must learn his or her roles and responsibilities for ensuring the Coast Guard remains secure and is able to maximize use of cyberspace to execute all missions.***

Current Threat Environment

- All organizations connected online—including the U.S. Coast Guard Auxiliary—are vulnerable to intrusions and disruptions from malicious actors
- Auxiliary IT systems and members have been the targets of a wide range of online attacks
  - Attempted Denial of Service and Probes originating from foreign nations
  - Credential theft from foreign IP's
  - Malicious code injected into CGAUX websites
  - Spear-phishing attempts against CGAUX members
  - Whaling attempts against CGAUX Commodores
- CGAUX is a target in today's threat environment
  - We are not in the .gov or .mil domain but our DHS/USCG affiliations expose us to the interest of those attacking the .gov/.mil domains
- Attacks are against CGAUX systems and individual member's personal accounts/systems
  - Vigilance remains a MUST



Cybersecurity Hygiene

- General Best Practices
- Passwords & Identity Management
- Social Media
- Website Usage
- Website Obfuscation
- Phishing / Spear-Phishing / Whaling
- Malware / Malicious Code
- Data on Mobile Devices
- Social Engineering
- Internet Hoaxes
- Wireless
- Identity Protection

General Best Practices

- Use passwords
  - Create separate accounts for each user
  - Create a passwords using a strong password creation method for each account
- Use current and supported operating systems
- Install all system security updates and patches
- Keep antivirus software up-to-date
- Regularly scan files for viruses
- Install spyware protection software
- Turn on firewall protection
- Change default logon ID and passwords for operating system and applications
- Change default logon ID and passwords for hardware such as rwireless access points, routers and cable modems
- Regularly back up and securely store your files
- Consider offsite or cloud backups

- Make sure your alerts are coming from the software you installed
  - Beware of sudden flashing pop-ups that warn that your computer is infected with a virus
  - This is a malicious code attack itself

Passwords & Identity Management

- For identity authentication, the Coast Guard and the Coast Guard Auxiliary are migrating towards two-factor authentication wherever possible. Two-factor authentication combines two out of the three types of credentials to verify your identity and keep it more secure:
  - Something you possess, such as an Auxiliary Logical Access Card (ALAC)
  - Something you temporarily have access to, such as the one-time passcode used in AUXDATA II
  - Something you know, such as your Personal Identification Number (PIN)
  - Something you are, such as a fingerprint or other biometrics

- Use two-factor authentication wherever possible, even for personal accounts
  - Many widely used personal services offer two-factor authentication

Passwords & Identity Management

- Create strong passwords both at work and at home:
  - Combine letters, numbers, and special characters
  - Do not use personal information
  - Do not use common phrases or dictionary words in any language
  - Do not write down your password - memorize it
  - Use a TRUSTED password manager
  - Do not save passwords on public machines
- Follow the system's policy on:
  - Password length
  - Frequency of changing your password
    - Best practice is at least every 3 months
  - Avoid using the same password between systems or applications
  - Minimum is not the best

Click Here To
Sign Up/In with
USCGAUX

Password Complexity

- How safe is your password?

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

Social Media

- Be aware of the information you post online about yourself and your family
  - Once you post content, it can't be completely taken back

- To protect yourself:
  - Understand and use the privacy settings
  - Create strong passwords
  - Don't give away your position through GPS or location links or updates about places where you are or where you will be
    - Post items after travel if necessary
  - If possible, validate friend requests before confirming them
    - Especially if you are already friends in the system
  - Beware of links to games, quizzes, and other applications available through social networking services
  - Avoid posting personally identifiable information (PII)

Social Media

- Social networking sites are not the only source of your online identity. Many apps and smart devices collect and share your personal information and contribute to your online identity. Examples are:
  - Fitness and health trackers
  - Professional networking apps
  - Dating apps and websites
  - Secure chat
  - Neighborhood advisory apps
  - Audio-enabled personal digital assistants (Siri & Alexa) and the smart devices they support, such as phones, TVs, and speakers
- Opt out of data aggregation if possible
- Use these apps and devices with caution

Website Usage

- A cookie is a text file that a web server stores on your hard drive. Cookies may pose a security threat, particularly when they save unencrypted personal information. Cookies also may track your activities on the web.
- To prevent cookies from being saved to your hard drive:
  - If you have the option, set your browser preferences to prompt you each time a website wants to store a cookie
  - Only accept cookies from reputable, trusted websites
  - Confirm that the site uses an encrypted link
    - Look for “h-t-t-p-s” in the URL name
    - o Look for an icon to indicate the encryption is functioning
  - Be especially aware of cookies when visiting e-commerce sites or other sites that may ask for credit card or other personal information
- Note: Not all https sites are legitimate and there is still a risk to entering your information online.

Website Obfuscation

- Make sure the website is what you expect
  - Beware of URLs with typos
  - Check that the domain makes sense
    - https://www.apple.com/appleID
    - https://appleID.sdjfhlsdjflksdjf.com/appleID
- Exercise caution with compressed URLs, such as TinyURLs (e.g., https://tinyurl.com/n213h)
  - Compressed URLs convert a long URL into a short URL for convenience but may be used to mask malicious intent
  - Investigate the destination by using the preview feature to see where the link actually leads
    - Use an Internet search engine to find instructions for previewing a specific compressed URL format

Email is Inherently Insecure

- An e-mail mailbox is not a secure storage system.
- E-mail is susceptible to eavesdropping in transit.
  - Transmissions are not necessarily encrypted.
  - Anyone who controls or can access network equipment between the servers (legitimately or not) may be able to intercept and read your e-mail.
- Even when encrypted transmissions, the encryption is not end-to-end.
  - At best, it's only encrypted during transmission between each e-mail server it visits in the path it takes from your device to your recipient. Not encrypted at rest by default.
- E-mail servers do not necessarily confirm the identity of the e-mail servers to which they connect to deliver messages.
- E-mail messages remain vulnerable to exposure long after delivery.
- E-mail messages can't be classified, restricted, assigned permissions, or otherwise protected by an administrator.
- Long e-mail conversations typically include all messages sent from the beginning of the conversation in each transmission, and, especially if the topic changes within the same thread, a user on the thread may forward it to a new recipient intending to share the most recent message or something recently attached.

Common Issue

Common BAD practice in Auxiliary: Send a password-protected document in one email. Send the password in a separate email.

- Send sensitive information out-of-band.
  - Especially critical for transmitting user credentials.
- Best scenario is to use a PKI enabled tool to sign and encrypt sensitive emails.
  - Digital Signature – Assures identity of sender
  - Encryption – Assures integrity of data

If communicating with USCG personnel,
ask to transfer PII/SPII/CUI using DoDSAFE.

DoD SAFE

Email Usage

- To prevent the downloading of viruses and other malicious code when checking your e-mail:
  - View e-mail in plain text and don't view e-mail in Preview Pane
  - Use caution when opening e-mail: Look for digital signatures if your organization uses them
  - Hover over links to see target
  - Be cautious of shortened links
- Use and trust digitally signed e-mails
  - Digitally sign emails with attachments or links
- Scan all attachments
  - If authenticity cannot be confirmed, delete e-mail from senders you do not know
  - Don't e-mail infected files to anyone
  - Don't access website links, buttons, and/or graphics in an e-mail or a popup generated by an email message

Phishing

- Phishing attempts use suspicious e-mails or pop-ups that:
  - Claim to be from your employer, government organization, Internet service provider, bank, or other plausible sender
  - Directs you to a website that looks real
  - Asks you to call a phone number to make any change to your computer, such as to help clean a virus from your computer
  - Claim that you must update or validate information
  - Threaten dire consequences
- Assume all unsolicited information requests are phishing attempts
  - Do not access sites by selecting links in e-mails or pop-up messages. Type the address or use bookmarks.
  - Contact the organization using a telephone number you know to be legitimate if you are suspicious of a link or attachment
  - Delete the e-mail
    - Report e-mails requesting personal information to appropriate security entity
  - Look for digital signatures
  - Never give out organizational, personal, or financial information to anyone by e-mail
  - Avoid sites with expired certificates. If officially directed to a site with expired certificates, report it to your security POC or help desk.

Phishing

- Spear phishing is a type of phishing attack that targets particular individuals, groups of people, or organizations. To protect against spear phishing:
  - Be wary of suspicious e-mails that use your name and/or appear to come from inside your organization or a related organization
  - Report the spear phishing e-mail to your security POC
- Be aware that high-level personnel may be targeted through complex and targeted phishing attacks called “whaling.” Whaling:
  - Is targeted at senior officials
  - Uses personalized information: name, title, official e-mail address, sender names from personal contacts lists
  - Is an individualized, believable message
  - Exploits relevant issues or topics
- To protect against whaling:
  - Be wary of e-mails that ask for sensitive information, contain unexpected attachments, or provide unconfirmed URLs
- Report the whaling e-mail

Phishing

Common Types of Phishing Attacks

PHISHING
The use of email to lure a victim into disclosing private information.

SPEAR PHISHING
Highly targeted phishing attack focused on specific individuals or groups of individuals.

WHALING
Spear phishing attack on high ranking officials or executives.

SMISHING
Phishing attempts to smartphones using SMS messages.

VISHING
Attacker contacts the victim by phone.

Phishing Tips

- **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical.
- **Research the facts**. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.
- **Don't let a link be in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.
- **Email hijacking is rampant.** Hackers, spammers, and social engineers taking over control of people's email accounts (and other communication accounts) has become rampant. Once they control an email account, they prey on the trust of the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.
- **Beware of any download.** If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.
- **Foreign offers are fake.** If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

Phishing Tips

- **Delete any request for financial information or passwords**
  - If you get asked to reply to a message with personal information, it's a scam.
- **Reject requests for help or offers of help**
  - Legitimate companies and organizations do not contact you to provide help.
- **Set your spam filters to high**
- **Secure your computing devices**
  - Install anti-virus software, firewalls, email filters and keep these up-to-date.
  - Set your operating system to automatically update.
  - Use an anti-phishing tool offered by your web browser or third party to alert you to risks.

Mobile Devices

- To protect data on your mobile computing and portable electronic devices (PEDs):
  - Lock your laptop/device screen when not in use and power off the device if you don't plan to resume use in the immediate future
  - Enable automatic screen locking after a period of inactivity
  - Encrypt all sensitive data on laptops and on other mobile computing devices when possible
  - At a minimum, password protect mobile computing devices; use two-factor authentication if possible
  - Configure devices to wipe data after a predetermined number of failed attempts (recommendation is 10)
  - Always maintain visual or physical control of your laptop and mobile devices and especially when going through airport security checkpoints
- When traveling with mobile computing devices, including laptops and cell phones:
  - Be aware that information sent over public Wi-Fi connections may be exposed to theft, and the device may be exposed to malware
  - Fake Wi-Fi access points may be used for deception
  - Use public or free Wi-Fi only with a VPN
- Use caution when connecting laptops to hotel Internet connections. If you are directed to a login page before you can connect by VPN, the risk of malware loading or data compromise is substantially increased.
- When traveling overseas with mobile devices:
  - Be careful and do not travel with mobile devices, unless absolutely necessary
  - Assume that any electronic transmission you make (voice or data) is monitored
  - Mobile phones carried overseas are often compromised upon exiting the plane

Wireless

- Wireless technology includes Bluetooth, infrared, wireless computer peripherals (e.g., wireless keyboard, wireless mouse, etc.), and smart devices (e.g., smart refrigerators, medical pumps, wireless-enabled hearing aids).
- To protect information systems and data on those systems:
  - Be cautious when using wireless technology
  - Ensure that the wireless security features are properly configured
  - Turn off/disable wireless capability when connected via LAN cable
  - Turn off/disable wireless capability when not in use
  - Avoid using non-Bluetooth paired or unencrypted wireless peripherals (e.g., keyboard, mouse, etc.)
- Wireless technology is inherently not a secure technology.

Internet of Things (IoT)

- Smart devices in your home, such as voice-enabled devices, enhanced remotes, smart thermostats, security cameras, and other programmable appliances, are part of what is known as the Internet of Things (IoT).
- These devices usually have a default (and sometimes unchangeable) password. This is one of their biggest security weaknesses.
- An unsecured IoT device could become an attack vector to any other attached devices. To secure IoT devices:
  - Examine the default security options available
  - Enable any security features
  - Set a robust password at the device's maximum length

Near Field Communication

- NFC is wireless technology that enables your personal electronic devices to establish communications and exchange information when placed next to each other. Smartphones can be enabled to:
  - Read electronic tag information, such as proximity cards or other objects with embedded NFC tags
  - Transmit information electronically, such as when making credit card payments with information held on the smartphone

- Security risks:
  - Eavesdropping: an adversary intercepts the signal
  - Data manipulation or corruption: an adversary intercepts the signal and alters it
  - Viruses: stored financial or mission information increases potential rewards for hackers

GPS Tracking

Many mobile devices and applications can track your location without your knowledge or consent. These devices can:

- Geolocation you
- Display your location
- Record location history
- Are often ON by default – sometimes even when your device is powered OFF

Stop and think before you wear or use a mobile device – Do you want your location shared?

Social Engineering

- Social engineers use telephone surveys, e-mail messages, websites, text messages, automated phone calls, and in-person interviews. To protect against social engineering:
  - Do not participate in telephone surveys
  - Do not give out personal information
  - Do not give out computer or network information
  - Do not follow instructions from unverified personnel

Internet Hoaxes

- Internet hoaxes clog networks, slow down internet and e-mail services, and can be part of a distributed denial of service (DDoS) attack. To protect against internet hoaxes:
  - Use online sites to confirm or expose potential hoaxes (SNOPES)
  - Don’t forward e-mail hoaxes
  - Follow your organization’s policies on loading files onto workstations and laptop

Disinformation

- Adversaries exploit social and other media to share and rapidly spread false or misleading news stories and conspiracy theories. Using accounts on popular social networking platforms, adversaries:
  - Disseminate fake news, including propaganda, satire, sloppy journalism, misleading headlines, and biased news
  - Share fake audio and video, which is increasingly difficult to detect as the creation technology improves
  - Gather personal information shared on social media to devise social engineering attacks
- To avoid being misled by disinformation:
  - Research the source to evaluate its credibility and reliability
  - Read beyond the headline
  - Check against known facts and other sources on the topic
  - Consider whether the story is intended as a joke
  - Check your personal biases

Identity Protection

- To protect your identity:
  - Ask how information will be used before giving it out
  - Pay attention to credit card and bank statements
  - Avoid common names/dates for passwords and PINs
  - Never share passwords and PINs
  - Pick up mail promptly
  - Do not leave outgoing postal mail in personal or organizational mailboxes, unless secured with a locking mechanism
  - Shred personal documents
  - Refrain from carrying SSN card and passport
  - Order credit report annually

- To respond to identity theft if it occurs:
  - Contact credit reporting agencies
  - Contact financial institutions to cancel accounts
  - Monitor credit card statements for unauthorized purchases
  - Report the crime to local law enforcement

Responsible AI Use

- Be cautious with personal data
  - Don’t feed sensitive info (SSNs, financials, work details) into AI tools
- Verify results
  - AI can hallucinate, or make things up
  - Always fact-check before sharing or acting
- Avoid harmful use (new regulations are and will continue to come into adoption)
  - Don’t use AI for deepfakes, disinformation, or impersonation
- Think before you share AI content
  - Treat AI outputs like any other online content
  - Check for accuracy, context, and source

Remember that Data Security is critical to AI Security - don’t forget security foundations

Secure Handling of USCG/CGAUX Data

- Removable Media in USCG Systems
- Use of US Government Email
- Security Policies for CGAUX Websites
- ALAC/NEATS Management

Removable Media in USCG Systems

- Removable media includes:
  - Flash media - thumb drives, memory sticks, and flash drives
  - External hard drives
  - Optical discs (such as CDs, DVDs, and Blu-rays)
- Other portable electronic devices (PEDs) and mobile computing devices, such as laptops, fitness bands, tablets, smartphones, electronic readers, and Bluetooth devices, have similar features.
- The same rules and protections apply to both.
  - Use only removable media approved by your unit
  - Only use flash media or other removable storage when operationally necessary, owned by your organization, and approved by the appropriate authority in accordance with policy
  - Do not use any personally owned/non-organizational removable media on your organization's systems
  - Do not use your organization's removable media on non-organizational/personal systems
  - Never plug unauthorized devices into a government system
  - Be aware that wireless connections to the devices bring increased threats and vulnerabilities

Removable Media in USCG Systems

- The risks associated with removable media include:
  - Introduction of malicious code
  - Compromise of systems' confidentiality, availability, and/or integrity
  - Spillage of sensitive information

Use of US Government Email

- E-mail use must not adversely affect performance of your role or reflect poorly on your organization. To use e-mail appropriately:
  - Do not use e-mail to sell anything
  - Do not send:
    - Chain letters
    - Offensive letters
    - Mass e-mails
    - Jokes
    - Unnecessary pictures
- Avoid using “Reply All” to prevent sending unnecessary e-mail traffic
- Only use e-mail for personal reasons if allowed by your organization
- Use a digital signature when sending attachments or hyperlinks, as required by DHS/USCG

Security Policies for CGAUX Websites

- Personally Identifiable Information (PII), such as addresses, phone numbers and email addresses, may only be displayed on WOW sites using WOW's protected pages or protected announcements, or on pages protected via the Member Zone login, unless the member has given specific permission to publish such information.
- No patrol schedules or radio frequencies may be shown on any Auxiliary web page, including on WOW protected pages or announcements.
- No Auxiliary web site may implement its own password protection system.
- Unencrypted documents (i.e., documents that are not password protected) that contain patrol schedules, Coast Guard radio frequencies or FOUO Information (For Official Use Only) may not be accessed on any web server. Any documents of this type can only be accessed on a web server if it is encrypted with a password that is changed periodically, and that password is sent to the intended reader separately (email delivery acceptable).
- Password protection of WOW protected pages is only to protect PII type info (e.g., email addresses or phone numbers), or non-sensitive information not of interest to the public.
  - No FOUO information can be displayed on any web site, including on WOW protected pages/announcements.
  - Patrol schedules or CG radio frequencies may not be displayed on WOW protected pages or announcements.
  - No links to unencrypted documents containing FOUO or patrol information.

ALAC/NEATS Management

- Auxiliary Logical Access Card (ALAC) and NIPRNet Enterprise Alternate Token System (NEATS) cards are variant of the DoD Common Access Card (CAC)
- The card is a controlled item. It implements DoD Public Key Infrastructure (PKI) and contains certificates for:
  - Identification
  - Encryption
  - Digital signature
- To protect your ALAC/NEATS:
  - Always maintain possession of your card
  - Remove and take your card whenever you leave your workstation
  - Never surrender or exchange your card for building access
  - If your card is lost or misplaced, report it immediately to your security POC
  - Store it in a shielded sleeve to mitigate card and chip cloning
  - Do not write down or share the PIN for your card
  - Do not allow commercial entities to photocopy or duplicate your card
- Lock your computer when you leave or shut it down, depending on your organization's security policy
- Do not use your card in unauthorized systems

Incident Reporting

- 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
- Any incident that meets the criteria above should be reported to an incident response center.

Incident Reporting

- 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 Cybersecurity Directorate (Y) http://wow.uscgaux.info/content.php?unit=Y-DEPT 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 Y Directorate 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 Y.
- 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 Y Directorate can be reached to assist with notifications, if necessary.

Conclusion

The security of the Coast Guard and Coast Guard Auxiliary information systems and data that we are entrusted with is all our responsibility. By securing and protecting our own personal IT resources that connect to USCG and CGAUX systems, we help to reduce the overall attack surface.

Reporting vulnerabilities and incidents is critical for protecting those systems. If you See Something or Suffer Something, make sure you Say Something so it can be Secured.

Phishing Incidents: phishing@cgauxnet.us

All Other Cybersecurity Incidents: cyber-incidents@cgauxnet.us