Initial New Hire Onboarding Security Guidance

Working in a Controlled Facility

As a Federally Funded Research and Development Center (FFRDC), MIT Lincoln Laboratory maintains a Department of Defense (DoD) Top Secret facility clearance. The Laboratory has a contractual relationship with the DoD that grants it access to classified information in order to conduct research and development in support of national security.

Various sponsors regularly assess the Laboratory for security compliance and its ability to properly safeguard classified information. In addition to properly safeguarding classified information in the interest of national security, a positive rating on these assessments are critical to maintaining the Laboratory's Top Secret facility clearance, contractual obligations, and continuity of business with the U.S. Government.

All Laboratory personnel must:

- Be able to obtain and maintain a security clearance as a condition of employment
- Accept personal responsibility for knowing, understanding, and adhering to Laboratory Security policies and procedures
- Safeguard sensitive unclassified and classified information
- All Laboratory personnel must support a safe working environment, free of violence or threats
- Have a favorably adjudicated commercial background investigation
- Properly use Laboratory IT systems and networks to limit risk

Hanscom Air Force Base enforcement of vehicle regulations

The Hanscom Air Force Base (HAFB) Security Forces Squadron has increased enforcement of vehicle regulations on Base and are authorized to issue citations within Laboratory parking lots and roadways. Laboratory personnel are reminded to adhere to the following traffic and parking regulations:

- Use ***hands-free*** phone devices only; texting while driving is prohibited
- Park in designated lined parking spaces only
    - Do not park in fire zones; loading zones; handicap parking areas
- Make a complete stop at all stop signs
- Observe all posted speed limits (Maximum of 10 MPH in parking lots and 25 MPH on HAFB)
- Yield to pedestrians entering crosswalks
- Use turn signals and seatbelts
- Vehicles are subject to searches at any time for prohibited items, such as:
    - Dash cameras and speed radar/laser detection units (if you possess one of these devices in your vehicle, they must be secured out of sight)
    - Firearms or ammunition (even if the individual has a license to carry)
    - Illegal substances (i.e. marijuana) and open alcoholic beverages
- Unregistered vehicles or drivers with expired licenses are not allowed to drive on HAFB
    - If inspection sticker is not current or has been rejected, your vehicle will not be allowed on HAFB
    - Proof of motor vehicle insurance and a valid driver's license is required to operate a vehicle on Base
- Motorcycles are subject to all applicable motor vehicle laws
    - All motorcycle operators on HAFB must wear appropriate protective clothing, head and eye protection, and sturdy footwear
    - Anyone riding a bicycle, scooter, and skateboard or roller blades on HAFB property is required to wear a helmet

Initial New Hire Onboarding Security Guidance

Prohibited and unauthorized items in Laboratory facilities

The following items are not authorized to be brought into Laboratory facilities:

- Photographic and recording equipment not approved by Laboratory policy (See section titled, “Bringing personally owned devices into Laboratory facilities”)
- Firearms, items that could be perceived as weapons, or ammunition
- Pyrotechnics, explosive substances or detonating devices
- Illegal substances (i.e. marijuana) and alcoholic beverages
- Gambling paraphernalia

Periodic unannounced inspections of personal effects such as briefcases, shoulder bags, handbags, luggage, athletic bags, boxes, packages, etc. will be conducted by the Security Services Department.

No expectation of privacy

- Laboratory computer systems are the property of the U.S. Government
- Users should not have an expectation of personal privacy in anything they create, store, send, or receive on Laboratory-owned computer systems or networks
- All electronic information and communications are subject to monitoring, recording, and management review
    - Electronic information and communications include, but are not limited to, email, voicemail, software, data, Internet access, computer sessions, computer connections, etc.
    - In reviewing electronic information and communications, management may take any actions deemed appropriate, including recording, copying, forwarding or transferring to others, erasure, or printing to protect the interests of the Laboratory and its U.S. Government sponsors
- Anyone utilizing Laboratory computer systems or networks expressly consents to such monitoring activities to conform to U.S. Government/DoD requirements

Bringing personally owned devices into Laboratory facilities

- Personally owned wireless and mobile devices (laptops, iPads, tablets, e-book readers, smartphones, smartwatches, two-way radios, fitness devices, and other devices with capabilities to electronically record, store, or transmit text, images, video or audio data) are only permitted within unclassified Laboratory areas where no classified processing, discussions, or meetings are in progress (e.g., Laboratory conference rooms and staff offices).
    - You must fill out a property pass for any personally owned laptops, iPads, tablets, and e-book readers
      Property passes are available at the Visitor Services Center.
- **Personally owned devices may not be connected to Laboratory systems or used to process Laboratory data or information**
    - Users are allowed to connect personally owned analog audio connector headsets with Tip Ring Sleeve (TRS) or Tip Ring Ring Sleeve (TRRS) to the analog headphone jack on the Laboratory system

- Camera, video, and recording functionality of personally owned devices may not be used within Laboratory facilities
- Mobile devices are subject to periodic, random content checks during compliance audits and inspections
    - Refusal to comply with requests for such reviews may result in management review and possible disciplinary action, to include termination

Use of social media

Lincoln Laboratory personnel are expected to demonstrate responsible use of social media (such as Facebook, Twitter, and LinkedIn) blogs, wikis, video- and photo-sharing sites, hosted services, web applications, and other social networking sites and applications. Unfavorable and sensitive information posted in these public forums may potentially cause damage to the Laboratory's reputation and research efforts.

Storing/processing Laboratory data

Laboratory personnel must never:

- Store or process Laboratory data on non-Laboratory owned systems or send data to non-Laboratory personal email accounts
- Store Laboratory data on unapproved cloud services (e.g., Google, iCloud)
- Post, disclose, or share Laboratory information in-person or telephone conversations, through email or text, on social media sites, or any other forms of communication that has not been approved for public release, including proprietary, sensitive, or classified information
- Disclose details about sensitive administrative budget information, meeting minutes reflecting program and planning decisions, announcements that include the time and location of classified or sensitive meetings or talks, details pertaining to sensitive or classified projects, detailed organization charts that contain technical areas of interest, Administrative and Security Procedures that contain policies or procedures that are not in the Laboratory’s best interest to be revealed to the public, and all administrative documents subject to but not yet approved for public release.
    - Resumes or job search web sites/apps should only contain information that is available in the public domain (basic job descriptions and information shared on the Laboratory external web site)

Guidelines to avoid social engineering and phishing attacks

Laboratory personnel are reminded to remain cautious of social engineering attacks that use human interaction to obtain or compromise information about the Laboratory or its computer systems. Phishing attacks—a form of social engineering—use email or malicious websites to solicit information by posing as a trustworthy source.

General guidelines to avoid being a victim of social engineering or phishing attacks:

- Do not open attachments or click on links contained in the body of suspicious email, or email sent from unknown senders
- Validate attachments and embedded links with the message sender prior to downloading the attachment or clinking on the link
- Validate the authenticity of internal Laboratory emails by verifying digital signatures
- Never reveal personal or financial information through email requests
- Never respond to suspicious emails

Initial New Hire Onboarding Security Guidance

- Identify indicators of suspicious email by looking for unusual attachment file names, poor grammar, and misspellings in the email subject, main body, or auto signature fields
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net)
- Do not give sensitive information to others unless you are sure that they are indeed who they claim to be and that they should have access to the information
- Be cautious when accessing personal web-based email accounts (e.g. Gmail) from Laboratory systems; these accounts do not provide the same level of security as the Laboratory's email service
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company
- Never give out personal information, such as logins and passwords, to anyone
- Never post information on blogs or social networking sites that can be used to target you or the Laboratory
- Never connect unknown or non-Laboratory electronic media to Laboratory equipment, unless otherwise stated in policy
- Always turn in found devices or unknown media to the Security Services Department

Common warning signs of a social engineering attack include:

- A request for protected information
- The unwillingness to leave a call-back number
- A show of discomfort when pressed for more information
- A high-pressure call at the end of the day/week with an urgent demand for information
- Name dropping, compliments, flattery, or flirting