Security Awareness Briefing for Contractors with Unescorted Entry and Without Active Directory Access

A. The Department of Interior (DOI) Departmental Manual (DM) 444 DM 1 states that all DOI employees and contractors with unescorted access must receive initial security awareness training within 60 days of being on-boarded and annually thereafter. The following excerpts are taken from the DOI Talent on-line security awareness training presentation and satisfies the requirements outlined in the above DM.

1. **OPERATIONS SECURITY (OPSEC)**. OPSEC is a process to deny potential adversaries critical information about capabilities and/or intentions by identifying, controlling, and protecting unclassified information that gives evidence of the planning and execution of sensitive activities. The following measures will help ensure good OPSEC practices.

   (a) Protect conversations/discussions concerning operational matters such as staffing, location of critical work areas, blueprints or security drawings, contracting information, security systems (their operation and locations), resource shortfalls, or maintenance issues to name a few.
   (b) Before sharing information, ensure the person(s) have a need to know and their employment status can be validated.
   (c) Be aware of your surroundings and those persons who might be suspicious.
   (d) If in doubt, contact your supervisor or a security professional.

2. **INFORMATION SECURITY (INFOSEC)**. INFOSEC focuses on the protection of classified and unclassified information. These categories of material can be in digital or hard-copy formats. The primary type of information you are likely to be exposed to is categorized as “Controlled Unclassified Information or CUI. This information is unclassified but documents or electronic media labeled as CUI is considered “sensitive” and its release or disclosure is based on a “need-to-know” basis and the validation that the person requesting the information is performing official government duties. The following guidelines will help ensure the proper handling and safeguarding of sensitive information and materials.

   (a) Protecting CUI is everyone’s responsibility.
   (b) Ensure sensitive information is protected such as in a locked drawer or room, and that the information is not left out on desks or in areas where casual passersby’s might have access to it.
   (c) Secure your computer or other electronic devices that may contain CUI information when unattended.
   (d) Safeguard all Personally Identifiable Information (PII) such as documents with personal addresses, social security numbers, dates of birth, etc.
   (e) Proper handling, storage, and dissemination guidelines can be found in SLE 02-01, *Identifying and Safeguarding Controlled Unclassified Information.*

3. **ACTIVE SHOOTER**. An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms. Below are recommendations to consider both before and during an active shooter event.

   (a) Be aware of your environment and familiar with entrances and exits.
   (b) Identify concealment areas and items that can be used as weapons or to help barricade doors.
   (c) Employ "Run, Hide, Fight."
      (1) "**Run**" away from the sounds of gunfire.
      (2) Leave personal belongings behind.
      (3) Do not stay behind because others refuse to leave.
      (4) "**Hide**" – use cover and concealment.
      (5) Hide your path and block your entrance.
      (6) Silence your phone and any other noise.
      (7) "**Fight**" when in imminent danger.
      (8) Without reservation, use any item as a weapon.
      (9) Aim for sensitive/vital areas such as face, nose, neck, groin, etc.

4. **Uncrewed Aircraft Systems (UAS)**. Uncrewed aircraft systems, formerly known as unmanned aerial/aircraft vehicles (UAV), or drones, are aircraft without a human pilot onboard that are controlled by an operator remotely or programmed to fly autonomously. UAS can pose a threat when operated by adversaries. They can cause disturbances, interfere with or disrupt operations, and possibly be used to create harm to personnel and damage to facilities. To enhance the safety and security of your site, facilities, and employees, practice the following procedures.

   (a) Report any UAS activity to your supervisor or security personnel.
   (b) Protect mission assets most vulnerable to a UAS threat.
   (c) Remain a safe distance away from the UAS. If the UAS is down, do not touch or handle it.
   (d) If possible, collect information such as location, description of the UAS, description of any individuals you see who might be operating the UAS, and a vehicle description (if applicable).

5. **Suspicious Persons/Activities.** Be situationally aware of your surroundings. If you see people in and around the facility or work site behaving in a suspicious manner or, you see an activity that appears suspicious, notify your supervisor or facility staff immediately. DO NOT approach or attempt to contact suspicious persons. If you believe the person or activity is serious or could cause damage to a facility or harm to you or other employees, call 911 and notify your supervisor.

B. Should you need to consult a security professional, contact your supervisor, project/facility/site manager, or a designated representative of the sponsoring organization.