Integrated Information Technology Solutions

Security Education & Training: Initial Orientation & Annual Refresher

Initial Orientation & Annual Refresher Security Education and Training is required per DoDM 5200.01, Vol. 3, Enclosure 5. This training provides basic security knowledge to recognize and respond to threats to National Security Information.

SEE SOMETHING, SAY SOMETHING

Agenda | Key Topics

- Need-to-Know
- Personnel Security
- Adjudications
- Continuous Vetting
- Periodic Reinvestigation
- Combination Controls
- Safeguarding Classified
- Storage Containers
- Top Secret Transmission
- Secret Transmission
- Confidential Transmission
- CUI Transmission
- Hand-Carry Requirements
- Levels of Classified Information
- Derivative Classification
- IS Marking Syntax
- Marking Slides & Working Papers
- Reproduction
- Destruction
- Processing Classified Information
- Controlled Unclassified Information
- IS Safeguarding
- Security Infractions / Violations
- Pre-Publication Process
- Public Media
- Industrial Security Program
- Physical Security Program
- OPSEC
- SEAD 3 Reporting Requirements
- Foreign Travel / Contact
- Insider Threat
- Foreign Recruitment
- Foreign Visits
- Active Shooter

NEED-TO-KNOW

Definition: Need-to-Know (NtK) is the determination by an authorized holder of classified information that another appropriately cleared individual requires access to the information in order to perform official duties.

Key Points:

- Signed Standard Form (SF) 312 "Classified Information Non-disclosure Agreement"
- Appropriate security clearance level
  - Your security clearance does not give you approved access to all classified information.
  - Possessing a badge that indicates a clearance does not automatically grant individuals a NtK.
- When working with other Contractors or Government Personnel, it is important to determine the degree of NtK BEFORE sharing project information.

Personnel Security

The Personnel Security Program: This program provides security policies and procedures; establishes the standards, criteria, and guidelines that personnel security determinations are based upon.

Position Designations:

- Special-Sensitive: Access to Sensitive Compartmented Information (SCI)/Top Secret (TS) or Special Access Program (SAP). Potential for *inestimable damage* to National Security.
- Critical-Sensitive: Access to Top Secret (TS). Potential for *exceptionally grave damage* to National Security.
- Noncritical-Sensitive: Access to Secret or Confidential. Potential for *significant or serious damage* to National Security.
- Non-Sensitive: No eligibility required. Does not pose damage to National Security.

Adjudications

- DOD Consolidated Adjudication Services (DOD CAS) is the primary authority for making security eligibility determinations for DOD personnel
- Utilizes whole person concept (looks at all available and reliable information about an individual's past and present prior to reaching an adjudicative determination)
- Uses 13 Adjudicative Guidelines

Personnel Security Adjudication

Continuous Vetting (CV)

- In accordance with DoDI 5200.02, “DOD Personnel Security Program (PSP)”
- For all personnel in national security positions
- Reviews background of individuals with access to National Security Information (NSI)
  - Additional or new checks of commercial databases
  - Government databases
- Determines if individual continues to meet eligibility requirements

Personnel Security Continuous Vetting (CV)

Periodic Reinvestigation

Tier 3R: Secret and Confidential

Reinvestigations will continue to be conducted every five (5) years.

Tier 5R: Top Secret (TS) or Sensitive Compartmented Information (SCI)

Reinvestigations will continue to be conducted every five (5) years with the Director of National Intelligence (DNI) endorsement.

Personnel Security Periodic Reinvestigation

Combination Controls

- Combinations which protect classified material shall be memorized, not written down.

- Combinations shall be changed upon initial issuance, when persons knowing the combination have been debriefed, when the combination is believed to have been compromised, or when otherwise deemed necessary by Security.

Safeguarding Classified

- When not in use, classified material shall be secured in a GSA-approved security container. Locking Bar containers are no longer authorized.
- A locked room, desk or file cabinet is not an approved method of classified storage.
- Containers shall be checked upon opening, closing, and at the end of the workday. End of Day checks shall be recorded and signed.

Storage Containers

GSA Approved Containers: Required for storing all classified materials

Standard forms to be completed:

- **SF700: Security Container Information**
  - ✓ Record combinations to security containers, secure rooms, and controlled area doors and to identify personnel to be contacted in an emergency
- **SF701: Activity Security Checklist**
  - ✓ Must be completed after all areas have been secured
- **SF702: Security Container Checklist**
  - ✓ Record date and time when opening or closing security container

Information Security
Top Secret Transmission

- **Authorized Transmit/Transport Methods for Top Secret or Top Secret/SCI Material**
  - Direct contact between cleared U.S. personnel
  - Protected secure communication system (facsimile, data, e-mail voice)
  - U.S. Transportation Command, Defense Courier Division
  - Appropriately cleared U.S. Military, Government and DOD contractor
- **Do Not Send Via**
  - U.S. Postal Service
  - *Overnight Express (FedEx)*

Information Security Secret Transmission

Transmit/Transport Secret

- Any of the means approved for the transmission of Top Secret information
- Appropriately cleared contractor employees if applicable
- U.S. Postal Service registered mail or express within U.S. and Puerto Rico
    - Check “Signature is Required” box
- U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service outside the U.S. and territories
    - Information may not pass out of U.S. citizen control
- Commercial delivery for urgent, overnight delivery only
- Open incoming packages immediately and secure

Information Security Confidential Transmission

Transmit/Transport Confidential

- Any of the means approved for the transmission of Secret information
- U.S. Postal Service certified mail to DOD contracting companies or non-DOD agencies
- U.S. Postal Service first class mail between DOD components in the U.S. and its territories
- Outer envelope marked “Return Service Requested”

DO NOT use external or street side mail collection boxes

Information Security
CUI Transmission

Transmit/Transport CUI

- U.S. Postal Service certified mail, parcel post, or fourth class mail
- Approved secure communications systems
- Avoid wireless telephone transmission of CUI when other options are available.
- Facsimile if appropriate protection is available at receiving location

Information Security Hand Carry

Hand-Carry Requirements

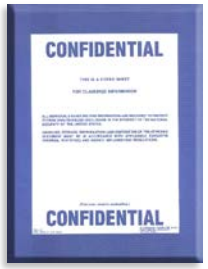
- Prepare inventory of material (one copy for your office and another with a responsible person)
- Double wrap material (lockable briefcase or zippered pouch may serve as outer wrapping and approved for carrying classified material)
- Receive courier briefing
- Carry courier card
- Carry courier letter (if transporting via commercial air)
- Keep under constant control
- Deliver to authorized person ONLY
- Trips that involve overnight stopovers are NOT permitted unless arrangements for storage in a U.S. Government office or a cleared contractor facility have been previously made.

Information Security Levels of Classified Information

All classified documents require a cover sheet. Classified media such as CDs, DVDs, hard drives, and thumb drives require medium tags or stickers.

Top Secret: Could cause exceptionally grave damage to national security that the Original Classification Authority (OCA) is able to identify or describe (SF703)

Secret: Could cause serious damage to national security that the OCA is able to identify or describe (SF704)



Confidential: Could cause damage to national security that the OCA is able to identify or describe (SF705)

DERIVATIVE CLASSIFICATION: Defined as incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

Derivative Classification Requirements

- Appropriate security eligibility
- Need-to-know
- Properly trained

Information Security Derivative Classification

Banner lines are at the top and bottom of the document and provide the overall classification of the document.

Portion markings denote the classification for each paragraph, sub-paragraph, or section in the document.

The Classification Authority Block (CAB) must include the name and position title or personal identifier of the DERIVATIVE classifier and, if not otherwise evident, the Component and office of origin, the source document or classification guide that the document was derived from, downgrade instructions if applicable, and the declassification date. The CAB must be on the face of the document.

Information Security Marking Syntax

Slide Presentations

- Mark first slide with overall classification marking
- Mark successive slides with either the overall classification or with the classification of the individual slide and portion markings for bullets
- Mark charts, graphics or figures by the classification of the portion, not of the chart/graphic/figure itself
- Classification authority block shall be placed on the first or last slide (less preferred)

Working Papers

- Mark with highest classification of any information contained in the document
- Date and annotate as “Working Papers”
- Destroy when no longer needed, remark within 180 days as a finished document or when released by the originator outside the originating activity

Information Security Marking Slides and Working Papers

Classified information shall be reproduced only to the extent required by operational necessity or for complying with applicable statutes or directives.

Reproduction Guidelines

- Use equipment approved at the appropriate level
- Ensure copies are subject to the same controls as original
- Limit reproduction to what is mission essential
- Ensure personnel are knowledgeable of the procedures for classified reproduction and aware of the associated risk involved with the specific reproduction equipment
- Comply with reproduction limitations
- Facilitate oversight and control

Information Security Reproduction

Classified material shall be destroyed completely to prevent anyone from reconstructing the information. The preferred method of destruction is shredding by using a National Security Agency (NSA) approved shredder.

Other Means of Destroying Classified Material

- Burning
- Wet pulping
- Mutilation
- Chemical decomposition
- Pulverizing

Destruction of Record and non-record CUI

- Same methods as classified
- Other methods that would not allow recognition or reconstruction
- Ensure law, regulation, or government-wide policy doesn't specify a specific method of destruction

Information Security Destruction

Rules for Processing Information: Use systems assessed or authorized to process information at the appropriate level.

Do Not

- Install software without approval
- Use another person's username and password
- Allow an unauthorized person to use your computer
- Circumvent or defeat security systems
- Permit unauthorized access to any sensitive computer network
- Modify or alter operating system configuration
- Write down your password

CLASSIFIED DOCUMENTS MUST BE RETRIEVED FROM THE PRINTER IN A TIMELY FASHION

Information Security Processing Classified Information

CUI: Unclassified information associated with a law, regulation, or government-wide policy and identified as needing safeguarding. Unauthorized disclosure of CUI could cause foreseeable harm.

Examples of CUI

- Investigation documents
- Inspection reports
- Agency budgetary information
- Procurement bids/proposals
- Personally Identifiable Information (PII)
- Information protected under Privacy Act of 1974

CUI DOES NOT INCLUDE CLASSIFIED INFORMATION

Information Security Controlled Unclassified Information (CUI)

Safeguard Classified Information (During/After working hours)

- General Services Administration (GSA) approved container vaults
- Secure rooms
- Secure telephone
- Maintain control, never leave unattended
- Do not talk around using codes or hints
- Do not divulge to unauthorized persons

Safeguard CUI

- Locked cabinets, file cabinets, bookcases
- Rooms with locked outer office doors
- Key or cipher locked rooms
- Similarly secured areas

Information Security Safeguarding

Security Infractions / Violations

A Security Incident can be categorized as an infraction or violation.

Infraction

- No loss or compromise of classified information
- Requires an inquiry to prevent a future violation but does not require an in-depth investigation

Violation

- Loss – information cannot be accounted for or physically located
- Compromise – Unauthorized disclosure of classified information to person(s) without valid clearance, authorized access, or need to know.
- Negligent Discharge of Classified Information (NDCI) – the unauthorized disclosure of classified data on an information system not authorized for the appropriate security level access controls.

Report ALL infractions and violations immediately to your Security Officer

Examples of Incidents

- Classified material not properly stored
- Classified container not properly secured
- Permitting personnel access to classified information without verifying need-to-know
- Failing to mark classified information
- Discussing classified information in unauthorized areas

For more information on security incidents refer to DoDM 5200.01 Vol. 3 available in the resources.

Sanctions

You are subject to sanctions if you knowingly, willfully, negligently:

- Disclose classified or CUI to unauthorized persons
- Classify information or continuing the classification of information in violation of DOD regulations

Sanctions include:

- Warning
- Reprimand
- Loss/denial of classified access
- Suspension without pay
- Termination of employment
- Discharge from military service
- Criminal Prosecution

You are responsible for protecting official information and complying with the pre-publication process

Materials subject to pre-publication review include:

- Books, manuscript, or articles sent to the publisher, editor, movie producer, or game purveyor, or their respective support staffs
- Speech, briefing, article, or content that will be publicly disseminated
- Information being released to the public, even through Congress or the courts
- Official government products as well as materials submitted by cleared or formerly cleared personnel.
- See DoDI 5230.29 “Security and Policy Review of DoD Information for Public Release” for more information.

The Defense Office of Prepublication and Security Review (DOPSR) is responsible for reviewing materials for public and controlled release.

Pre-Publication Process

Classified Information in the Public Media

- Do not confirm or deny
- Do not respond to questions about programs or projects including those released through:
    - Radio or TV
    - Newspapers
    - Magazines
    - Trade journals
    - Social media sites, such as Facebook, Twitter, Pinterest, or LinkedIn
- Do not view or download from unclassified IT systems. Make a note of the URL and other significant details.

Refer all questions to the Public Affairs Office (PAO) and your Security Officer

Information Security Classified Information/Public Media

Industrial Security Program

Working with Contractors

- Contractors may or may not be cleared
  - Verify eligibility through a valid visit authorization request or system of record
  - Cleared under National Industrial Security Program (NISP)
  - Follow requirements of the National Industrial Security Program Operating Manual (NISPOM)
  - Required to comply with your organization's security program

Check with your security office for information on verifying contractor employee clearance eligibility and need to know.

Physical Security Program

Physical Security:

Active and passive measures to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.

Physical Security Countermeasures:

- Barriers/Fencing establish boundaries and deter individuals
- Intrusion Detection System (IDS) is used to deter, detect, document, deny, or delay intrusion by detecting a change in the environment.
- Security forces are made up of DOD, military, contract personnel, and trained dogs
- Lighting is used to deter intruders for fear of being seen

Physical Security Employee Identification

Homeland Security Presidential Directive 12 (HSPD-12) Common Access Card (CAC)

- DOD wide form of identification
- Used by civilians, contractors, and military personnel
- Contains personal identifying data and Public Key Infrastructure (PKI) certificate
- Used for email encryption, digital signing, and network access

If your CAC card is either lost or stolen, report it to your security office immediately.

Physical Security Escort Requirements

Escort Requirements

- Ensure access to controlled areas by non-cleared personnel is minimal
- Only cleared personnel who are familiar with the security procedures of the facility are authorized to escort non-cleared personnel
- Ensure all visitors sign the Visitor Log upon entry

Operations Security (OPSEC)

OPSEC: Process of protecting critical information that can be used against us by preventing our adversaries access to information and actions that may compromise an operation.

OPSEC Practices:

- Remove ID badge when leaving your facility and secure it in a safe place
- Loss of any form of ID should be reported IMMEDIATELY to your security office
- Do not post or send sensitive information over the web
- Guard against calls to obtain sensitive information
- Do not discuss sensitive information in public, or over an UNCLASSIFIED phone line
- Watch for and report suspicious activity

Security Executive Agent Directive 3 (SEAD 3) Reporting Requirements

Individuals in the federal government with access to classified information should be aware of established reporting requirements or hold sensitive positions.

SEAD 3 implementations may vary for industry, DOD departments and agencies.

Reporting requirements for ALL covered individuals include Foreign Travel, Foreign Contacts and Reportable Actions by Others.

Report ALL activities to the FSO immediately.

Personnel Security Self-Reporting

IF YOU DON'T SELF REPORT, SOMEONE ELSE MIGHT.

Self-Reporting

- Report changes in:
  - Status: Marriage, co-habitation, addition of new family member, divorce, receipt of large sum of cash
  - Adverse Information:
    - Criminal activity (domestic violence, issuance of restraining order)
    - DUI/DWI
    - Traffic tickets over $300
    - Excessive indebtedness, financial difficulties, bankruptcy
    - Use of illegal drugs
  - Foreign Contacts and Foreign Travel

See The Security Executive Agent Directive 4 for more information. Reporting does not automatically result in revocation of eligibility, so don't be afraid to report!

Security Executive Agent Directive 3 (SEAD 3) Reporting Requirements

Individuals With Access to Secret or Confidential Information, “L” access, or holding a Noncritical-sensitive

Foreign Activities:

- Application for and receipt of foreign citizenship
- Application for, possession, or use of a foreign passport or identity card for travel

Other Activities:

- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified or other “protected” information
- Media contacts, other than for official purposes, where the media seeks access to classified or otherwise “protected” information, whether or not the contact results in an unauthorized disclosure
- Arrests
- Bankruptcy or over 120 days delinquency on any debt
- Alcohol or drug-related treatment Position
- Cryptocurrency - foreign state-backed, hosted, or managed cryptocurrency

Security Executive Agent Directive 3 (SEAD 3) Reporting Requirements

Individuals with Access to Top Secret Information, “Q” access, or holding a Critical-sensitive or Special-sensitive Position

Foreign Activities:

- Direct involvement in foreign business
- Foreign bank accounts
- Ownership of foreign property
- Foreign citizenship
- Application for and receipt of foreign citizenship
- Application for, possession, or use of a foreign passport or identity card for travel
- Voting in a foreign election
- Adoption of non-U.S. citizen children

Security Executive Agent Directive 3 (SEAD 3) Reporting Requirements

Individuals with Access to Top Secret Information, “Q” access, or holding a Critical-sensitive or Special-sensitive Position

Other Activities:

- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified or other information specifically prohibited by law from disclosure regardless of means
- Media contacts where the media seeks access to classified or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure
- Arrests
- Financial anomalies
- Foreign national roommate(s)
- Cohabitant(s)
- Marriage
- Alcohol or drug-related treatment
- Cryptocurrency - foreign state-backed, hosted, or managed cryptocurrency

Foreign Travel Official

All cleared personnel must provide advance notice of foreign travel plans to their Security Office and receive approval prior to foreign travel.

Foreign Travel Requirements:

- Obtain defensive foreign travel security briefing prior to travel or at least once a year
- Obtain country specific briefing from the Counterintelligence Office (if required)
- Antiterrorism/Force Protection Level 1 training completion must be current
- Contact nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer if detained or subjected to harassment or provocation

Overseas Travel increases the risk of being targeted by foreign intelligence activities. The foreign intelligence services have better access to you and their actions are not restricted when they are operating within their own countries. Information Age spying includes:

- Wired hotel rooms
- Interceptions of fax and email transmissions
- Recording of telephone calls/conversations
- Bugged airline cabins
- Unauthorized access and downloading, theft of hardware and software. Do not put phones and laptops in checked bags
- Break-ins and/or searches of hotel rooms, briefcases, and luggage

Foreign Travel

COMPUTER SECURITY

Another area of concern while traveling is computer security. Foreign Intelligence Services are not usually fortunate enough to have information simply dropped into their hands. They rely on tactics such as stealing laptops. These portable systems may contain access capabilities that serve as doorways to additional information and systems. In addition to theft, travelers have reported unauthorized access, attempted access, damage and evidence of surreptitious entry of their portable electronic devices.

Foreign Travel

Foreign Travel SCI

SCI indoctrinated personnel planning foreign travel, personal or officially must follow the previous steps in addition to:

- Complete a foreign travel questionnaire prior to travel
- Provide complete copy of itinerary
- Be aware of nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer
- Upon arrival from travel, complete return questionnaire

Foreign Contact Reporting

All cleared personnel must report foreign relationships to their Security Office. SEAD 3 requires that all unofficial contacts be reported if the contact:

- Is Continuing
- Involves bonds of affection, personal obligation, or intimate contact
- Involves the exchange of personal information

This reporting requirement is based on the continuing association with the foreign national, regardless of whether the relationship has continued in person, online or via mail.

Reportable Contact By Others

SEE SOMETHING, SAY SOMETHING

All cleared personnel should report any activity that raises doubt whether another employee's continued national security eligibility is clearly consistent with the interests of national security.

The following activities must also be reported:

- Unexplained affluence or excessive indebtedness
- An unwillingness to comply with rules and regulations
- Suspected mental health issues
- Illegal use of drugs
- Excessive alcohol consumption
- Criminal conduct

Insider Threat

Potential Espionage Indicators

- Attempt to conceal oversees travel or contact with foreign nationals
- Seeking to gain higher clearance or expand access outside the job scope
- Engaging in classified conversations without a NtK
- Working hours inconsistent with job assignment or insistence on working in private
- Exploitable behavior traits
- Repeated security violations
- Attempting to enter areas not been granted access to

Not every person who exhibits one or more of these indicators is involved with illicit behavior, but most of these persons who have been involved with espionage were later found to have displayed one or more of these indicators.

Insider Threat

Reportable Behaviors

- Obtaining access to sensitive information inconsistent with present duty requirements
- Keeping classified materials in an unauthorized location
- Attempting to access sensitive information without authorization
- Using an unclassified medium to transmit classified materials
- Removing classification markings from documents
- Sudden reversal of financial situation or a sudden repayment of large debts or loans
- Attempting to conceal foreign travel
- Repeated or un-required work outside of normal working hours

Foreign Recruitment

WHAT IS RECRUITMENT

An intelligence definition of recruitment is the attainment of someone's cooperation to provide sensitive or classified information, usually after careful assessment and patient cultivation of the target by an intelligence service. By the time the "pitch" (the offer to work for the foreign government) is made, the intelligence officer (the "recruiter") is relatively confident of the target's willingness to cooperate. If a failed recruitment attempt is reported, serious consequences may result for the involved Intelligence Officer (IO).

Foreign Visits

International visits are a common part of everyday business in today's international market/economics and are a welcome opportunity to boost any business. The cleared Department of Defense (DoD) Contractor is no exception to this growth in the International Market. Visits to DoD Cleared Contractors by foreign delegations and individuals have been noted as one of the most frequently utilized modus operandi for targeting US Defense Industry for the past five years.

TECHNIQUES

- **Peppering** – Several of the visitors asking the same question in different styles or one visitor asking the same question to multiple US Contractor employees.
- **Wandering visitor** – The visitor uses the distraction provided by a large delegation to slip away, out of control of the escort.
- **Divide and Conquer** – The foreign visitors take the team members into different areas to discuss issues, thus, relieving the US person of his safety net of being assisted in answering questions or eliminating oversight of what he releases.
- **Switching visitors at the last minute** – A tool that is sometimes used to add a collector to the group without leaving enough time for a background check to be performed on the new visitor.
- **Bait and Switch** – The delegation says they are coming to discuss business that is acceptable for discussion, but after they arrive their agenda switches to different questions and discussions.
- **The distraught visitor** – When the visitor does not have questions answered he/she has a temper tantrum or acts as though they are insulted, thereby trying to get the US person to answer the questions and not be upset.

Foreign Visits

Active Shooter

What is an Active Shooter

- Active Shooters are individuals who attempt to injure or kill people in confined and populated areas
- Common threads are random victim selection and no clear advanced planning (in most cases)
- Average incidents last 10-12 minutes
- Most casualties happen in the first 3 minutes
- 63% are employees of which 18% were fired that day

Indicators in the workplace

- Repeated policy violations
- Talk of financial problems
- Depression / withdrawal
- Explosive outbursts of anger without provocation
- Paranoid behavior
- Escalation of domestic problems into workplace
- Talk of previous incidents of violence

Choices that you may need to make

- Run/Evacuate – Always have an escape route or plan in mind and leave your belongings behind
- Hide/Shelter in Place – Silence your cell phone and turn off other sources of noise
- Fight/Take action against shooter – Act as aggressive as possible against shooter (you are all in or not at all)

Info to provide law enforcement officer or 911 operator

- Location of active shooter
- Number of shooters
- Physical description of shooters
- Number and type of weapons
- Number of potential victims at the location

Active Shooter

Completed Security Training

- Need-to-Know
- Personnel Security
- Adjudications
- Continuous Vetting
- Periodic Reinvestigation
- Combination Controls
- Safeguarding Classified
- Storage Containers
- Top Secret Transmission
- Secret Transmission
- Confidential Transmission
- CUI Transmission
- Hand-Carry Requirements
- Levels of Classified Information
- Derivative Classification
- IS Marking Syntax
- Marking Slides & Working Papers
- Reproduction
- Destruction
- Processing Classified Information
- Controlled Unclassified Information
- IS Safeguarding
- Security Infractions / Violations
- Pre-Publication Process
- Public Media
- Industrial Security Program
- Physical Security Program
- OPSEC
- SEAD 3 Reporting Requirements
- Foreign Travel / Contact
- Insider Threat
- Foreign Recruitment
- Foreign Visits
- Active Shooter

Summary

Integrated Information Technology Solutions

Please take the Security Quiz and fill in the Training Certificate information. Let the Facility Security Officer (FSO) know if you have any questions.