UCF | Office of Research and Commercialization

UNIVERSITY OF CENTRAL FLORIDA

ANNUAL SECURITY REFRESHER & INSIDER THREAT TRAINING

Table of Contents

Office of Research and Commercialization
UCF | UNIVERSITY OF CENTRAL FLORIDA

Introduction

WELCOME!

I am Dela Williams, Facility Security Officer (FSO) at the University of Central Florida. I would like to welcome you to your Annual Security Refresher Briefing and Insider Threat Training.

If you were asked, “Who is responsible for security?” how would you answer? I hope you would answer, I am responsible for the reason that, as a cleared U.S. citizen, UCF cleared employee, and serve as a vital part on the national’s security team each and every day. You play a critical role in protecting classified information and following other security requirements.

The threats to our national’s resources and information continue to emerge and multiple. Some threats are in the cyber arena, including spear-phishing, viruses, and malware. Others are more traditional, such as theft and foreign and economic espionage. It is vital that you are alert to both the technical, non-technical threats, and familiar with the protective measures you can take.

Additionally, it is important to be aware of the policies and processes in place to ensure we remain compliant with government regulations concerning the protection of classified information.

This annual briefing was developed to increase your awareness and sharpen your security skills while you serve as an integral member of our national’s security team. If you have any questions about the material covered in this training or any other security concerns, please contact me immediately.

Thank you for your continued participation in your security responsibilities.

Dela Williams

Facility Security Officer
University of Central Florida
Office of Research and Commercialization

What is the NISPOM
REQUIREMENTS?

The U.S. government has established detailed requirements which are outlined in the National Industrial Security Program Operating Manual (NISPOM) to ensure the protection of classified information.

The National Industrial Security Program Operating Manual (NISPOM) **3-108. Refresher Training.** The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. See paragraph **8-103c** of chapter 8 of this Manual for the requirement for IS security refresher training. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

NISPOM Reference:
8-103c. All IS users will:
(1) Comply with the ISs security program requirements as part of their responsibilities for the protection of ISs and classified information.
(2) Be accountable for their actions on an IS.
(3) Not share any authentication mechanisms (including passwords) issued for the control of their access to an IS.
(4) Protect authentication mechanisms at the highest classification level and most restrictive classification category of information to which the mechanisms permit access.
(5) Be subject to monitoring of their activity on any classified network and the results of such monitoring could be used against them in a criminal, security, or administrative proceeding.

3-103b. Insider Threat Training. All cleared employees must be provided insider threat awareness training before being granted access to classified information, and annually thereafter. Training will address current and potential threats in the work and personal environment and will include at a minimum:
(1) The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.
(2) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within ISs.
(3) Indicators of insider threat behavior, and procedures to report such behavior.
(4) Counterintelligence and security reporting requirements, as applicable.

Security Clearance Eligibility

Whenever a Department of Defense (DoD) employee or contractor requires access to classified national security information (and/or assignment to a national security sensitive position), the individual must be granted security clearance eligibility at the proper level to access that information or occupy the national security sensitive position.

A security clearance eligibility is a determination that a person is able and willing to safeguard classified national security information and/or occupy a national security sensitive position. The three national security clearance eligibility levels are: Confidential, Secret, and Top Secret.

A prerequisite for accessing classified national security information and/or assignment to a national security sensitive position is completion and favorable adjudication of a national security background investigation.

The investigation is non-criminal and covers a defined period of normally no more than the last 10 years. The information collected must be sufficient to allow an affirmative or negative determination of a person's eligibility for access to classified information and/or assignment to a national security sensitive position.

The adjudicative process is the careful weighing of a number of variables known as the "whole person concept." Available, reliable information about the individual (past and present, favorable and unfavorable) is considered in reaching a determination of eligibility.

Eligibility for access is granted only when facts and circumstances indicate that access to classified information or assignment to a national security sensitive position is consistent with the national security interests of the United States.

What is
SECURITY CLEARANCE ELIGIBILITY?

A security clearance is a determination that you are eligible for access to classified information and/or eligible to hold a national security sensitive position.

Not everyone is granted a favorable security clearance eligibility. Only those reasonably determined not to be a national security risk are granted eligibility and permitted to handle classified information and/or hold a national security position.

The purpose of security clearance eligibility is to determine whether you are able and willing to safeguard classified national security information or hold a national security sensitive position, based on your loyalty, character, trustworthiness, and reliability.

What is
CLASSIFIED INFORMATION?

Classified information is official information or material that requires protection in the national interest.

Classified information is national security information, which means that it relates to the national defense and foreign relations of the United States.

If classified information is mishandled or given to the wrong person, it could harm our country's security or that of our allies.

You will learn more in the Information Security section.

What is a
NATIONAL SECURITY SENSITIVE POSITION?

National security sensitive positions are designated positions that do not require access to classified information but require performing sensitive duties related to national security.

If these duties are performed by an untrustworthy individual, there is a potential for harm to national security.

Some examples include the need to access restricted areas, sensitive DoD equipment, or information technology (IT) systems.

Why do we
NEED SECURITY CLEARANCES?

We need security clearances to ensure that only trustworthy people have access to classified information and/or hold national security sensitive positions.

Common sense and personal experience tell us that not all people are equally trustworthy.

The security clearance process is a tool that helps make sure national security information is not given to people who cannot be trusted.

POSITION DESIGNATION

Within the DoD, each civilian position is categorized, with respect to security sensitivity, into one of four groups:

- Special Sensitive
- Critical Sensitive
- Non-Critical Sensitive
- Non-Sensitive

SPECIAL SENSITIVE positions involve the following:

- Access to **Sensitive Compartmented Information (SCI)** Tier 5 (T5) investigation is conducted.
- Positions that could cause immeasurable damage to the national security and/or immeasurable compromise to technologies, plans, or procedures vital to the strategic advantage of the United States

CRITICAL SENSITIVE positions involve the following:

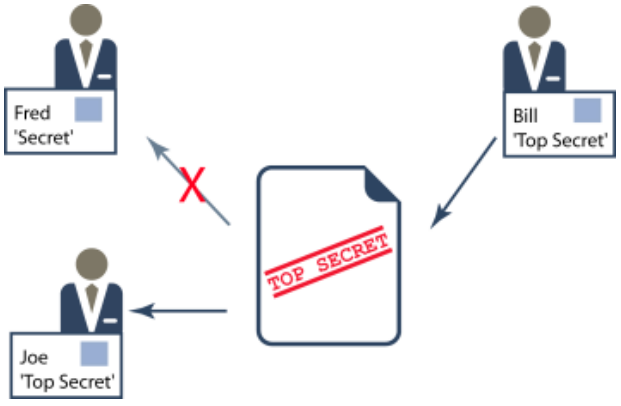
- Access to **Top Secret** information. Tier 5 (T5) investigation is conducted.
- Positions which have the potential to cause exceptionally grave damage to the national security

NON-CRITICAL SENSITIVE positions typically involve the following:

- Access to **Secret or Confidential** information. Tier 3 (T3) investigation is conducted.
- Positions which have the potential to cause significant or serious damage to the national security

NON-SENSITIVE positions:

- All other positions are designated as non-sensitive
- Non-sensitive positions do not require access to classified information or assignment to national security sensitive duties



Obtaining Eligibility

Once I receive my eligibility,

CAN I ACCESS *ANY* CLASSIFIED INFORMATION?

No! Access to any classified information depends on the level of clearance eligibility you have (Confidential, Secret, or Top Secret) and the information you need to know to do your job. This is called the **"need-to-know"** principle.

- With a Confidential clearance eligibility, you have access solely to that ***Confidential*** information you actually need-to-know to do your job.
- Similarly, a ***Secret*** clearance eligibility enables access to Secret and Confidential information on a need-to- know basis.
- A ***Top Secret*** clearance eligibility enables access to Top Secret, Secret, or Confidential information that you actually need-to-know to do your job.

The organization's management (supervisor, manager, or designated representative) determines what classified information you need access to in order to get your job done.

"need to know"

What are my Access

REQUIREMENTS?

Clearance Eligibility + Signed SF-312 + Need-to Know = Authorized Access

Clearance – Administrative action, usually involving a form of background investigation.

SF-312 – Signed Non-Disclosure Agreement

is a legally binding document and remains in effect whether or not you are working on a classified contract for-the-rest of your life. In signing the SF312, you have agreed to never disclose classified information to which you have been given access.

Need-to-know – A determination made

that access to classified information is necessary in order to perform tasks or services essential to the fulfillment of a classified contract or program.

Until you are granted a FINAL clearance, you may not have access to:

- Restricted Data (RD)
- COMSEC Information (COMSEC)
- NATO Information (NATO)

Additionally, you must receive specialized briefings from Security for any access to Special Programs (SAP/SAR), plus:

-Restricted Data (RD)
-COMSEC
-NATO
-Foreign Travel
-CI
-WNINTEL
-Courier

Counterintelligence/ Threat Awareness

What is the THREAT?

United States cleared industry is a prime target of many foreign intelligence collectors and foreign government economic competitors. Cleared employees working on America's most sensitive programs are of special interest to other nations. The number of reported collection attempts rises every year, indicating an increased risk for industry.

The nature and extent of industry reported suspicious contacts suggest a concerted effort to exploit cleared contractors for economic and military advantage. These contacts range from outright attempts to steal technology to seemingly innocuous business ventures.

One of the fastest growing areas of concern is the exploitation of cyberspace for surreptitious access to cleared contractor data systems and cleared individuals. The potential for blended operations where cyberspace contributes to traditional tradecraft presents the greatest risk to cleared industry. An increase in unsolicited contacts made with cleared industry employees from compromised accounts amplifies the potential for compromise of cleared individuals, classified programs, or classified systems occurring in the unclassified cyber domain.

You are the frontline of defense against these threats. Being alert to the threat and reporting suspicious activity contributes to helping our national security.

Report Suspicious Activities

to Dela Williams,

Insider Threat Program Senior Official (ITPSO)

What is ACADEMIC SOLICITATION?

Defense Security Service defines academic solicitation as the use of students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or classified information.

These attempts can include requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations; requests to study or consult with faculty members; requests for and access to software and dual-use technology; or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees.

COUNTERINTELLIGENCE Video

What are possible
COLLECTION METHODS?

Requests for Information
This is the most frequently reported collection method and provides the greatest return for minimal investment and risk. Collectors use direct and indirect requests for information (e.g. e-mails, phone calls, conversations) in their attempts to obtain valuable U.S. data. These types of approaches often include requests for classified, sensitive, or export-controlled information. A simple request can gain pieces of information helpful in uncovering a larger set of facts

Solicitation or Marketing of Services
Foreign-owned companies seek business relationships with U.S. firms that enable them to gain access to sensitive or classified information, technologies, or projects

Acquisition of Technology
Collectors continue to exploit direct and indirect acquisition of technology and information via third parties, the use of front companies, and the direct purchase of U.S. firms or technologies

Public Venues
Conferences, conventions, symposiums and trade shows offer opportunities for foreign adversaries to gain access to U.S. information and experts in dual-use and sensitive technologies

Official Foreign Visitors and Exploitation of Joint Research
Foreign government organizations, including intelligence and security services, consistently target and collect information through official contacts and visits

Cyber Attack
Cyber threats are increasingly persistent and rapidly becoming a primary means of obtaining economic and technical information. Reports of new cyber-attacks against U.S. government and business entities continue to increase. Adversaries have expanded their computer network operations, and the use of new venues for intrusions has increased

Mobile Telephones
Threats against mobile phones continue to rise. Smart phones such as Blackberry and iPhone, essentially general purpose computers, are susceptible to malicious software, according to open source reporting

Foreign Targeting of U.S. Travelers Overseas
Foreign collectors also target U.S. travelers overseas. Collection methods include everything from eliciting information during seemingly innocuous conversations, to eavesdropping on private telephone conversations, to downloading information from laptops or other digital storage devices

Targeted Information and Sectors
Foreign collectors continue to seek a wide range of unclassified and classified information and technologies from specific targets. Information systems attract the most attention; aeronautics, lasers and optics, sensors, and marine systems are other top targets

Insider Threat

Who is an INSIDER? – What is INSIDER THREAT?

Insider: Any person with authorized access to any government or contract resource to include personnel, facilities, information, equipment, networks or systems. This can include employees, former employees, consultants, and anyone with access.

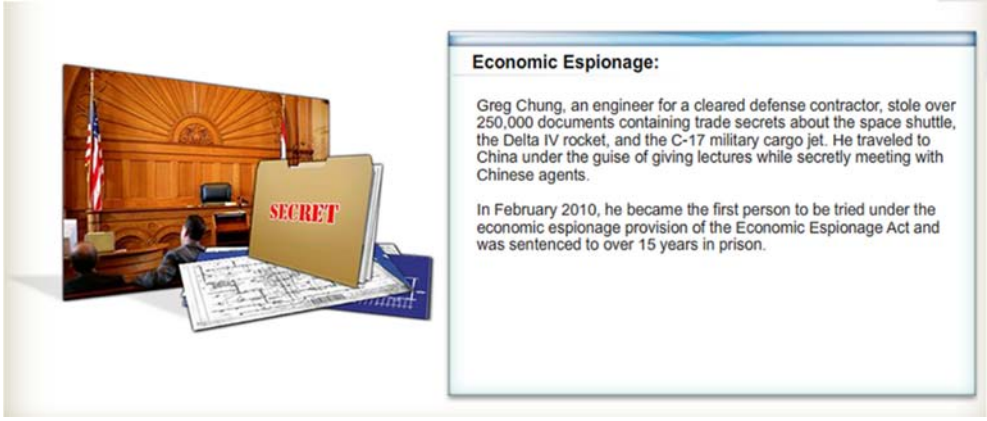
Insider Threat: The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of government, company, contract or program information, resources, or capabilities.

Why is the Insider Threat SIGNIFICANT?

An insider can have a negative impact on national security and industry resulting in:

- Loss or compromise of classified, export-controlled, or proprietary information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Physical harm or loss of life

Insider Threat Case Study



How can YOU HELP?

You are the first line of defense against insider threats. Help protect our national security by reporting any suspicious behavior that may be related to an insider threat.

Each employee has a responsibility to ensure the protection of classified and controlled sensitive information entrusted to them.

Be aware of potential issues and the actions of those around you and report suspicious behaviors.

How to
RECOGNIZE AN INSIDER THREAT?

Detecting potential malicious behavior among employees with access to classified or controlled sensitive information involves gathering information from many sources and analyzing that information for clues or behaviors of concern. In most cases, co-workers admit they noticed questionable activities, but failed to report incidents because they did not recognize the pattern or did not want to get involved or cause problems for their co-workers.

A single indicator may say little; however, if taken together with other indicators, a pattern of behavior may be evident.

Ignoring questionable behaviors can only increase the potential damage the insider can have on national security or employee safety. While each insider threat may have different motivation, the indicators are generally consistent.

INSIDER THREAT Video

What are some Indicators
POTENTIAL ESPIONAGE?

- Repeated security violations and a general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals when required to do so
- Seeking to gain higher clearance or expand access outside the job scope without bona fide need for the access
- Engaging in classified conversations without a need to know
- Attempting to enter areas not granted access to
- Working hours inconsistent with job assignment or unusual insistence on working in private
- Accessing information not needed for job

BEHAVIORAL*?

- Depression
- Stress in personal life
- Exploitable behavior traits:

  – Use of alcohol or drugs
  – Gambling
- Financial trouble
- Prior disciplinary issues at work

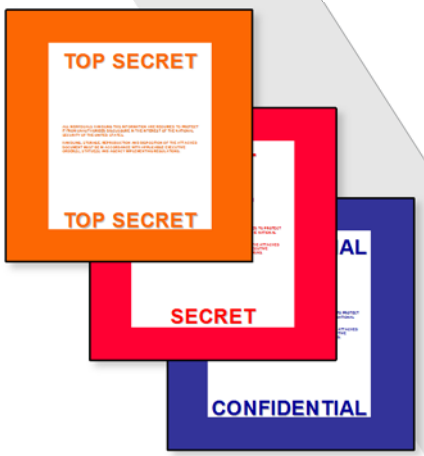
**These behaviors may also be indicative of potential workplace violence.*

Information Security

Classified Information is sensitive information which belongs to the U.S. Government and to which access is restricted by law or regulation to people who do not possess the right level of clearance and a need-to-know, in the interest of National Security.

Information Security pertains to the protection of classified and controlled unclassified information (CUI) from unauthorized disclosure, including, but not limited to:

- Marking
- Handling
- Transmission
- Storage
- Destruction



How is INFORMATION CLASSIFIED?

ORIGINAL CLASSIFICATION - An original classification decision at any level can be made only by a U.S. Government official who has been delegated the authority in writing.

DERIVATIVE CLASSIFICATION

Contractors who do one of the following are making derivative classification decisions:

- Extract or summarize classified information
- Apply classification markings derived from a source document, or
- Are directed by a classification guide or a contract security classification specification (DD254)

LEVELS OF CLASSIFICATION

Classified information must be appropriately marked to alert recipients of the information's classification level

There are three (3) levels of classification

- CONFIDENTIAL (C) - unauthorized disclosure of CONFIDENTIAL information could be expected to cause **Damage** to National Security.
- SECRET (S) - unauthorized disclosure of SECRET information could be expected to cause **Serious** Damage to National Security.
- TOP SECRET (TS) - unauthorized disclosure of TOP SECRET information could be expected to cause **Exceptionally Grave** Damage to National Security
- UNCLASSIFIED is not a classification level, but is a designation indicating that the item or content is not classified.

What Information can be CLASSIFIED?

Does the information fall within one of 8 eligible categories?

Military plans, weapons systems, or operations	Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
Foreign government information (FGI)	U.S. Government programs for safeguarding nuclear materials or facilities
Intelligence activities (including covert action), intelligence sources or methods, or cryptology	Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security.
Foreign relations or foreign activities of the United States, including confidential sources	Development, production, or use of weapons of mass destruction

Information shall not be classified, continue to be maintained as classified, or fail to be declassified in order to:

Conceal violations of law, inefficiency, or administrative error	Restrain competition
Prevent embarrassment to a person, organization, or agency	Prevent or delay the release of information that does not require protection in the interest of national security

Limitations on classification apply to certain types of information:

Basic scientific research information not clearly related to national security shall not be classified	Information not previously disclosed to the public under proper authority may be classified or reclassified if it meets the requirements of E.O. 13526
Information may not be reclassified after declassification and release to the public under proper authority, except under certain conditions	

Types of Material, includes, but not limited to:

Machinery	Reproductions
Documents	Storage Media
Emails	Working Papers
Models	Sketches
Faxes	Maps
	Photographs

What is CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI is unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, and Government-wide policy.

Departments and agencies within the U.S. Government assign different CUI designations.

CUI designations include, but are not limited to the following. You are obligated to protect them from disclosure and misuse:

- For Official Use Only (FOUO)
- Law Enforcement Sensitive (LES)
- Sensitive But Unclassified (SBU)
- Unclassified information related to a classified program
- Personally-Identifiable Information (PII) (e.g., SSN, DOB, POB)

How do you SAFEGUARD CLASSIFIED INFORMATION?

Must be under the positive control by an authorized person or stored in a locked security container, vault, secure room, or secure area	Must receive appropriate training prior to performing derivative classification duties and receive refresher training every two years thereafter
Must respect and understand the markings and the downgrade/declassification instructions on classified material	Discuss or send via secure communications
Discuss in an area authorized or appropriate for classified discussion	Process on approved equipment
	Destroy by approved methods

SANCTIONS

You may be subject to criminal, civil or administrative sanctions if you knowingly, willfully, or negligently:

- Disclose classified information to unauthorized persons
- Classify or continue the classification of information in violation of DoD regulations
- Create or continue a Special Access Program (SAP) contrary to the requirements of DoD regulations
- Disclose controlled unclassified information (CUI) to unauthorized persons
- Violate any other provision of applicable DoD regulations

Sanctions may include, but are not limited to:

- Warning
- Reprimand
- Loss or denial of classified access
- Criminal prosecution
  - Persons who commit espionage with classified or export-controlled data will be prosecuted and can receive substantial fines (up to $5,000,000) and jail time (up to 20 years) and may even be subject to the death penalty in the case of classified compromise!
  - Companies can receive fines up to $10,000,000! Plus get debarred from applying for government work
- Removal from employment
- Discharge from military service
- Suspension without pay

Adjudicative Guidelines

How is the SECURITY DETERMINATION MADE?

When a DoD military, civilian, or contractor's investigation is complete, it is sent to the DoD Consolidated Adjudications Facility (CAF).

An adjudicator at the DoD CAF will review all of the information, both "good" and "bad" (remember, the "whole person") and assess the information against the National Security Adjudicative Guidelines.

- If there is no information that raises a security concern, the individual will usually be granted a favorable security clearance eligibility at the level requested by their agency.
- If there is information that raises a security concern, the adjudicator will evaluate the adverse information and mitigating factors per the National Security Adjudicative Guidelines when making the eligibility determination.
- If significant adverse material is identified, the case may be delayed until additional information is gathered and facts are verified. Ultimately, an unfavorable security clearance eligibility determination may be made if the adverse information cannot be mitigated.

What are
ADJUDICATIVE GUIDELINES?

The **13 Adjudicative Guidelines** for determining eligibility for access to classified information and eligibility to perform national security sensitive duties are:

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

Due Process

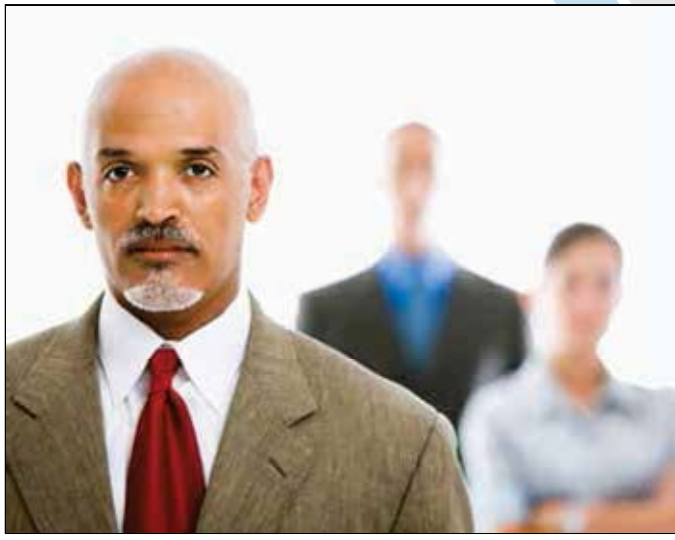
Security clearance eligibility can be denied only on the basis of substantive information that raises doubts regarding trustworthiness. It is never denied on the basis of gender, race, religion or sexual orientation.

DoD has gone to great lengths to ensure that the security clearance eligibility process is fair and balanced.

A security clearance eligibility is not denied without an individual being given the opportunity to explain or rebut the adverse information.

This is called due process, and it includes essential appeal rights, which individuals can exercise to challenge security clearance eligibility denials or revocations to an independent appeal board.

These rights include the option to either present a written appeal directly to the board or to make a personal appearance before a DoD administrative judge that will be considered by the board in its independent decision.



CYBERSECURITY

Cybersecurity prevents damage to, protects, and restores information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

Information Systems include, but are not limited to:

- Computers
- Electronic communications systems/services
- Handheld devices that provide computing, telephone/fax, Internet and networking features (e.g., Blackberry, iPhone, iPad, Android)

SOCIAL MEDIA Video

ANTITERRORISM

Antiterrorism includes defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces.

Additionally, antiterrorism includes actions taken to prevent or mitigate hostile actions against personnel (including family members), information, equipment, facilities, activities, and operations.

SURVIVING AN ACTIVE SHOOTER Video

OPSEC

Operations Security (OPSEC) is a systematic process that is used to mitigate vulnerabilities and protect sensitive, critical, or classified information

OPSEC Video

Continuous Evaluation

Once the initial adjudication decision has been made and as long as you are assigned to a national security sensitive position or have access to classified information or material, you will fall under the Continuous Evaluation Program (CEP).

By definition, the CEP involves the uninterrupted assessment of a person for retention of a security clearance eligibility or continued assignment to a national sensitive position. This ensures that high standards of conduct are maintained and that questionable conduct or activities are promptly reported for adjudicative assessment.

In the near future an automated records check monitoring system will be put in place to cover the gap between the initial investigation and the periodic reinvestigation (PR).

CEP also includes reinvestigation at given intervals based on the types of duties you perform and clearance eligibility level.

- Individuals in **Critical Sensitive** positions are reinvestigated every five years (Tier 5 Reinvestigation/T5R) if they have access to **Top Secret**
- Those in **Non-Critical Sensitive** positions (Tier 3 Reinvestigation/T3R) are reinvestigated every 10 years if they have access to **Secret** material, and every 15 years if the access is to **Confidential** information. However, under the new Federal Investigative Standards (FIS), the reinvestigation interval for secret and confidential eligibility will transition to five years by October 2017

Obligation

My security clearance eligibility, WHAT ARE MY OBLIGATIONS?

- When you hold security clearance eligibility, or hold a national security sensitive position, you are expected to comply with the high standards of conduct required of persons having access to classified information or performing national security sensitive duties. See "Personal Conduct."
- You are expected to keep your security office informed of certain changes in your personal life or activities in which you engage that have potential security ramifications. See "Self-Reporting of Personal Activities."
- You are also expected to report any factual information that comes to your attention and that raises potential security concerns about co- workers. See *"Reporting Responsibilities."*

Standards of conduct are set by Executive Order 12968 on Access to Classified Information. That presidential order directs that access to classified information is granted only to individuals "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information."

Failure to comply with the standard may cause your security clearance eligibility to be reviewed and possibly revoked.

The concept of continuing evaluation is an important part of the personnel security process. It means you are subject to periodic reinvestigation and to a reasonable degree of monitoring by supervisors, co-workers, and security professionals between investigations. These safeguards are necessary because situations and behaviors change over time. Experience shows that individuals granted eligibility to access classified information or occupy a sensitive position, sometimes fall into a pattern of unreliable or untrustworthy behavior after being granted an initial eligibility.

Self-Reporting

SELF-REPORTING OF PERSONAL ACTIVITIES

Although you may obtain security clearance eligibility or may be assigned to a national security sensitive position, the initial adjudicative decision can be overturned at a later date if you concealed relevant information during the investigation or after the eligibility was issued.

Employees who have access to classified information or occupy a national security sensitive position are expected to report changes or incidents that may impact their security clearance eligibility.

The Adjudicative Guidelines can be a valuable tool in determining if a life-event or situation might result in a need to report. "Although self-reporting is mandatory, it also demonstrates personal integrity and is preferable to the incident or change being discovered and reported by others.

The following are some examples of incidents and life events where reporting certain changes is expected or may be appropriate.

- **CHANGE IN PERSONAL STATUS:** Marital status (marriage, divorce), cohabitation (living in spouse-like relationship, intimate relationship, or becoming engaged), change of name, citizenship (even if dual)
- **FOREIGN TRAVEL:** A security briefing is required before any foreign travel, whether for personal or business reasons, clearance for travel to hazardous countries for *Sensitive Compartmented Information (SCI) cleared individuals.*

Specific Threats to Travel Destination:
U.S. Department of State information: http://travel.state.gov/

Contact the Facility Security Officer to verfty required training and reporting requirements.

- **FOREIGN CONTACTS:** Contact with individuals of any foreign nationality, either within or outside the scope of your official duties, in which illegal or unauthorized access to classified or otherwise sensitive information is sought, personal concern that you are a target of an attempted exploitation, all close and continuing relationships between SCI-cleared individuals and foreign nations.

- **LOSS OR COMPROMISE OF INFORMATION:** Inadvertent or accidental loss or compromise of classified or other sensitive information.
- **FINANCIAL PROBLEMS:** Filing for bankruptcy, garnishment of wages, having a lien placed on your property for failing to pay a creditor, eviction from a residence for failure to pay rent, or simply your inability to meet all your financial obligations.
- **ARRESTS:** Any arrest, regardless of whether or not charges were filed, other involvement with the legal system (such as being sued), any circumstance where you were sworn under oath to testify about your association or involvement in questionable activities.
- **PSYCHOLOGICAL OR SUBSTANCE ABUSE COUNSELING:** Self-reporting is appropriate for psychological treatment unless it is for marital, family, or grief counseling, not related to violence by you, or strictly related to adjustments from service in a military combat environment, or you were a victim of sexual assault who sought counseling for an emotional or mental health condition strictly in relation to the sexual assault.

  Seeking help for life's stressors does not reflect adversely on an individual's judgment. Instead, it may be viewed as a positive sign that an individual recognizes that a problem exists and is willing to take responsible steps toward resolving it.
- **OUTSIDE ACTIVITIES:** Any planned or actual outside employment or volunteer activity that could create a real or apparent conflict with your designated job duties.
- **MEDIA CONTACTS:** Any media inquiries about your job or organization should be reported: ongoing personal contacts with media representatives who cover your organization or your subject specialty should be cleared with security.
- **PRE-PUBLICATION REVIEW:** Any technical paper, book, magazine article, or newspaper article that you prepare for publication or for posting on the Internet, or lecture or speech that you prepare to give, must be cleared in advance if it contains information or knowledge you gained during your current or any previous job.

SECURITY ISSUES

The next section lists examples of behaviors that may indicate an individual has vulnerabilities that are of security concern or that an individual is in need of assistance. This list is developed from the Federal Adjudicative Guidelines.

You should consider reporting these behaviors when observed, so that your supervisor or the security office can determine whether some type of preventive or investigative action is appropriate.

If ignored, problems signaled by these behaviors could impair the health, well-being, or performance of the individual employee, disrupt the work unit, or lead to compromise of sensitive information.

Early intervention is often the key to quick, effective resolution of problems with minimal or no impact to the individual or the organization.

Because an individual exhibits one or more of the following behaviors does not mean he or she is a security risk. A security judgment is based on a pattern of behavior, and not a single action. And, it is a whole person judgment that takes many factors into account, including strengths as well and weaknesses.

The list of security-relevant behaviors is not a checklist for you to collect information on your co-workers. It simply provides examples of behaviors that may signal an individual is having problems or may need assistance. Consider the list, along with everything else you know about the individual and the sensitivity of the individual's position, and then exercise your best judgment in determining whether to report, and what, when, and to whom to report.

BEHAVIORS THAT ARE POTENTIAL SECURITY CONCERNS

The following are examples of behaviors that may indicate an individual has vulnerabilities of a security concern or that an individual is in need of assistance.

This list of behaviors is not all-inclusive. The list is not a statement of Government policy, but simply illustrative of the kinds of behaviors that may be considered when a person is under consideration for a security clearance or a position of trust. Some behaviors are obviously more significant than others.

ALCOHOL CONSUMPTION

- Alcohol-related incidents at work, such as reporting to work or duty in an intoxicated or impaired condition, or drinking on the job
- Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use
- Habitual or binge consumption of alcohol to the point of impaired judgment

ALLEGIANCE TO THE UNITED STATES

- Actual or threatened use of force or violence in an effort to change Government policy, prevent Government personnel from performing their assigned duties, or prevent others from exercising their constitutional rights
- Known participation in any organization or group advocating or threatening use of force of violence, as above

CRIMINAL CONDUCT

- Theft
- Fraud (for example, bribery or solicitation of bribes, misuse of a Government credit card, misuse of leave, fraudulent travel or expense accounting, or tax fraud)
- Pattern of disregard for rules and regulations (in addition to theft and fraud, this includes taking classified information home at night, or driving while intoxicated)
- Spouse or child abuse or neglect
- Attempts to enlist others to participate in illegal or questionable activity

DRUG INVOLVEMENT

- Use, possession, or acquisition of illegal/illicit substances including marijuana, whether it is legal in your locality or not
- Misuse (use other than as prescribed), inappropriate possession, or inappropriate acquisition of prescription medication

FINANCIAL CONSIDERATIONS

- Living or spending beyond one's means
- Unexplained affluence (unusually large or lavish purchases) or sudden large sums of cash that may indicate illegal source of income
- Calls at work from creditors
- Bounced or bad checks
- Garnishments, repossessions, unfavorable judgments, or other indications of financial difficulty
- Failure to make child or spousal support payments
- Reckless or compulsive spending, extensive gambling losses, or gambling debt
- Bankruptcy
- Improper handling of official finances or property, including repeated delinquent accountings for advances, and unexplained cash
- Shortages or loss of property, sloppy handling of cash funds, and disregard for financial or property administration regulations

PSYCHOLOGICAL CONDITIONS

- Pattern of significant change from past behavior, especially relating to increased nervousness or anxiety, unexplained depression, hyperactivity, decline in performance or work habits, deterioration of personal hygiene, increased friction in relationships with co-workers, isolating oneself by rejecting any social interaction
- Expression of bizarre thoughts, perceptions, or expectations
- Pattern of lying and deception of co-workers or supervisors
- Talk of or attempt to harm one's self
- Argumentative or insulting behavior toward work associates or family to the extent that this has generated workplace discussion or has disrupted the workplace environment
- Exploitation or mistreatment of others through intimidation or abuse of power or position
- Other disruptive workplace behavior that resists supervisory direction or counseling
- Verbal or physical threats toward work associates or family
- Inability to control anger — throwing things, acts of violence
- Stalking-type behavior (such as unwanted following, harassing phone calls, or online bullying)
- Extreme or recurrent statements of bitterness, resentment, vengeance, or disgruntlement that suggest a risk of some illegal or improper action
- Threats or attempts to get even with work associates, acts of vindictiveness

FOREIGN INFLUENCE

- Unreported personal contacts with personnel from a foreign intelligence service, foreign government, or persons seeking classified, proprietary, or other sensitive information
- Unreported close and continuing contact with a foreign national, including intimate contacts, shared living quarters, or marriage
- Unreported relatives, or unreported contact with relatives, in a foreign country
- Unreported relationship between relative, associate, or person sharing living quarters and any foreign government, foreign intelligence service, criminal or terrorist group, or group advocating disloyalty toward the United States

FOREIGN PREFERENCE

- Exercising benefits of dual citizenship, including possession and use of a foreign passport or other foreign identify documentation without approval
- A deeply held commitment to helping a foreign country or group that an individual that may show a preference over the U.S. or be tempted to circumvent U.S. policy or security regulations to assist the foreign country or group

USE OF INFORMATION TECHNOLOGY SYSTEMS

- Unauthorized entry into any compartmented computer system
- Unauthorized searching/browsing through classified computer libraries
- Unauthorized modification, destruction, manipulation, or denial of access to information residing on a computer system
- Unauthorized introduction of media into any Government computer system
- Storing or processing classified information on any system not explicitly approved for classified processing
- Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research

OUTSIDE ACTIVITIES

- Failure to report paid or volunteer work for any U.S. or foreign media, publisher, academic institution, research organization or corporation relating to the topics on which one has access to classified information

PERSONAL CONDUCT

- Recurring pattern of poor judgment, irresponsibility, or emotionally unstable behavior
- Deliberate omission or falsification of material information about background when applying for security processing
- Association with persons involved in criminal activity
- Indications subject may succumb to blackmail rather than risk exposure of a personal issue

HANDLING PROTECTED INFORMATION

- Persistent lax security habits despite management counseling (such as discussing classified information on non-secure phone, not properly securing classified information or areas, or working on classified material at home)
- Collecting or storing classified information outside approved facilities
- Revealing of classified information to unauthorized persons, including news media
- Inappropriate, unusual, or excessive interest in classified information outside of one's need-to-know
- Statements or actions that demonstrate an individual believes the security rules do not apply to him/her

SEXUAL BEHAVIOR

- Pattern of self-destructive or high-risk sexual behavior that the individual is unable to stop
- Criminal sexual behavior

DEFENSE HOTLINE

NISPOM 1-208. Federal agencies maintain hotlines to provide an unconstrained avenue for contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects:

Defense Hotline
The Pentagon
Washington, DC 20301-1900
800-424-9098

YOUR SECURITY CLEARANCE ELIGIBILITY IS A CONTINUING RESPONSIBILITY!

Are you able and willing to safeguard classified national information or perform national security sensitive duties? Your loyalty, character, trustworthiness, and reliability will determine your qualification to hold a security clearance eligibility or sensitive position. Your continued diligence in monitoring your behavior and responsibly dealing with life's events will help you maintain your eligibility for a security clearance or occupancy of a national security sensitive position. Should you have any questions, contact me Dela Williams at dela.williams@ucf.edu or (407) 882-1123.

Course Completion

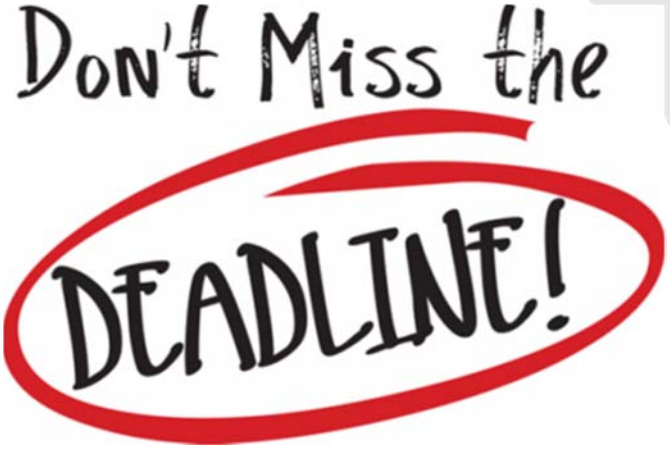
Now that I have completed the course,
HOW DO I GET CREDIT FOR TAKING THIS COURSE?

To acknowledge you have taken this course please follow the below instructions:

- Read the statement on the Annual Security Training Briefing 2017 Acknowledgment Receipt.
- Sign, Print your Name, and Date Completed

- Send an email to Dela Williams, FSO at dela.williams@ucf.edu on the same day of completion of the course

Acknowledgment Receipt is due April 30th



UNIVERSITY OF CENTRAL FLORIDA

Office of Research and Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246

Annual Security Training Briefing 2018

Acknowledgment Receipt

I acknowledge receiving "UCF's Annual Security Briefing" by the Office of Research and Commercialization which described my continuing responsibility to safeguard classified information. I understand that my signature below affirms I understand the contents of the Annual Security Briefing and Insider Threat Training.

Employee Signature: _____

Employee Printed Name: _____

Date: _____

The National Industrial Security Program Operating Manual (NISPOM) **3-108. Refresher Training.** The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. See paragraph **8-103c** of chapter 8 of this Manual for the requirement for IS security refresher training. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

NISPOM Reference:
8-103c. All IS users will:
(1) Comply with the ISs security program requirements as part of their responsibilities for the protection of ISs and classified information.
(2) Be accountable for their actions on an IS.
(3) Not share any authentication mechanisms (including passwords) issued for the control of their access to an IS.
(4) Protect authentication mechanisms at the highest classification level and most restrictive classification category of information to which the mechanisms permit access.
(5) Be subject to monitoring of their activity on any classified network and the results of such monitoring could be used against them in a criminal, security, or administrative proceeding.

3-103b. Insider Threat Training. All cleared employees must be provided insider threat awareness training before being granted access to classified information, and annually thereafter. Training will address current and potential threats in the work and personal environment and will include at a minimum:
(1) The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.
(2) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within ISs.
(3) Indicators of insider threat behavior, and procedures to report such behavior.
(4) Counterintelligence and security reporting requirements, as applicable.