UCF | Office of Research and Commercialization

UNIVERSITY OF CENTRAL FLORIDA

INITIAL SECURITY TRAINING

TABLE OF CONTENTS

Acknowledgment	2
Introduction	3
Reporting Requirements	5
Procedures and Duties	7
Safeguarding Reproduction	8
Transmission	8
Retention/Disposition	8
Classification Overview	10
Insider Threat	11
Counterintelligence	12
Conclusion	13
Completing the Non-Disclosure Agreement	13
Glossary	14

ACKNOWLEDGMENT

You have been granted a Department of Defense (DoD) security clearance and consequently the U.S. government has provided authority for you to access certain classified information.

As a recently cleared individual for the University of Central Florida, there are basic security concepts you will need to learn. This initial security training will provide you with foundational knowledge, expectations, and requirements you will need to understand prior to beginning work on any classified information, data, material, or restricted or closed areas.

Thank you,

Dela Williams

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

INTRODUCTION

INDIVIDUAL SECURITY RESPONSIBILITIES

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. Part of your role as a cleared University of Central Florida employee is to protect our nation from a variety of threats. Our National Security is constantly under attack by adversaries both foreign and domestic; by protecting classified information, you are fulfilling a critical role in protecting our nation.

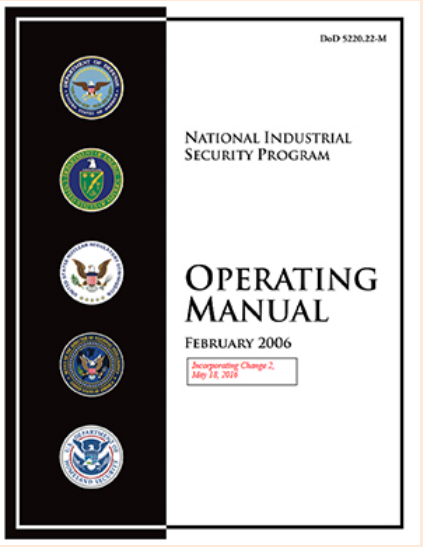
This initial security training will provide security procedures that are critical for cleared employees to understand and comply with government security regulations. Although each cleared facility adheres to set government security standards, implementation procedures may vary from site to site.

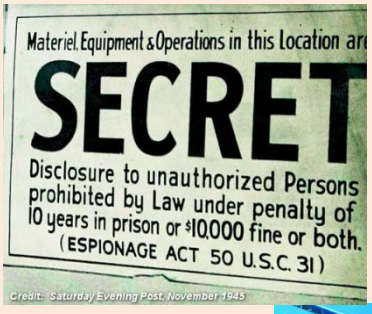
PENALTIES

Penalties for unauthorized disclosure of classified information, which can be assessed against both cleared employees and the organization, include:

- Criminal, Civil, and Other Measures
- Fines of up to $10,000+
- Imprisonment of up to 10+ years

For defense contractors such as UCF, Defense Security Service (DSS) is the primary DoD security agency assigned to oversee the protection of classified information.





INTRODUCTION (CONT)

NISPOM 3-107. Initial Security Briefings. Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:
a. A threat awareness security briefing, including insider threat awareness in accordance with paragraph **3-103b** of this Manual.
b. A counterintelligence awareness briefing.
c. An overview of the security classification system.
d. Employee reporting obligations and requirements, including insider threat.
e. Initial and annual refresher cybersecurity awareness training for all authorized IS users (see chapter 8, paragraph **8-101c**, of this Manual).
f. Security procedures and duties applicable to the employee's job.

NISPOM Reference:
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.

8-101c. ISs Security Program. In addition to the training requirements outlined in paragraphs **3-107** and **3-108** of chapter 3 of this Manual, all IS authorized users will receive training on the security risks associated with their user activities and responsibilities under the NISP. The contractor will determine the appropriate content of the security training taking into consideration, assigned roles and responsibilities, specific security requirements, and the ISs to which personnel are authorized access.

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.

8-103c. Contractor Responsibilities. 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.

REPORTING REQUIREMENTS

Cleared employees have a number of reporting requirements you must adhere to in order to maintain your security clearance. These reporting requirements are centered on events and activities that could potentially impact your ability to protect classified information.

CHANGE IN PERSONAL STATUS

- Name
- Citizenship including acquiring dual citizenship and/or foreign passports
- Residence
- Marital status
- Cohabitation in a spouse-like relationship with a foreign national
- Job assignment no longer requiring a security clearance

SUSPICIOUS CONTACT

- Any contact with an individual that is suspicious in nature, whether they are a U.S. or foreign person
- Someone taking an unusual interest in you and your job and/or asking probing questions about what you do and who you work for

These contacts can occur online, through social media, email, via-phone, written correspondence, or in-person.

Some examples of suspicious contacts include:

- Request for protected information under the guise of a price quote or purchase request, market survey, or other pretense
- Attempts to entice cleared employees into situations that could lead to blackmail or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export license on file
- Attempts to place cleared personnel under obligation through special treatment, favors, gifts, or money

These reports should be made to the Facility Security Officer or Designated Security Representative and if you are in doubt as to whether something is reportable.

ADVERSE INFORMATION

You must also report information that reflects unfavorably on the integrity or character of yourself or another cleared individual that may impair the ability to safeguard classified materials. This information is defined as adverse information.

Some examples of adverse information include:

- Known or suspected violation of security rules by you or another individual
- Known or suspected compromise of classified information by you or another individual
- Any arrest, criminal activity, or civil court actions
  - Traffic fines over $300 (not including court fees)
- Treatment for psychological, mental, emotional, and personality disorders and counseling, *except* family/marriage, grief and combat-related counseling (unless the counseling was precipitated by a violent action or event)
- Substance abuse
- Medical marijuana (prior to use)
- Use of illegal controlled substances (which includes marijuana under federal law)
- Unexplained affluence
- Excessive indebtedness or recurring financial difficulties (e.g., foreclosure or bankruptcy)
- Knowledge of an employee not wanting to perform on classified work
- Close or continuous contact with a foreign person or entity
- Misuse of any company or U.S. government information systems
- Behavior causes an individual to be vulnerable to coercion, exploitation, or duress and/or reflects lack of discretion or judgement (to include behavior of a sexual nature)

REPORTING REQUIREMENTS (CONT)

FOREIGN TRAVEL

Foreign travel increases the risk of foreign intelligence targeting. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you, and their actions are not restricted within their own country's borders**.**

You may possess or have access to information that is highly sought after by foreign entities, including:

- Friendly information
- Research, development, testing, and evaluation
- Program milestones and specifications
- System capabilities

Foreign entities also target information related to your organization's personnel, security, and operations.

A favored tactic for industrial spies is to attend trade shows and conferences. This environment allows them to ask questions, including questions that might seem more suspect in a different environment. One assessment estimated that one in fifty people attending such events were there specifically to gather intelligence.

Specific Threats to Travel Destination:

U.S. Department of State information:
http://travel.state.gov/

Crime is one of the biggest threats facing travelers. Crimes against travelers are crimes of opportunity.

Follow these steps to protect yourself:

- Stay alert and exercise good judgment
- When possible, ensure that your hotel room has a peephole and a deadbolt lock or a chain-and-slide bolt
- If you travel with valuables, put them in the hotel safe
- Find out what parts of town locals consider risky and avoid them
- Keep your car doors locked and suitcases out of sight
- If you see an accident, don't stop; instead, call for help from a safe area
- Minimize the amount of cash you carry
- Be wary of street vendors and innocent-looking youngsters as they may be decoys for pick pockets

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.

LOSS OR COMPROMISE OF INFORMATION

If you inadvertently or accidentally lose or compromise classified or other sensitive information, this must be reported.

OUTSIDE ACTIVITIES

Any planned or actual outside employment or volunteer activity that could create a real or apparent conflict with your designated job duties.

PROCEDURES AND DUTIES

LEVELS OF CLASSIFIED INFORMATION

The United States government has three levels of classified information. The level of classification is determined by the degree of negative impact to National Security if improperly disclosed. The classification levels are defined as:

- **CONFIDENTIAL** - This classification is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause **damage** to National Security.
- **SECRET** - This classification is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause **serious damage** to National Security.
- **TOP SECRET** - This classification is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause **exceptionally grave damage** to National Security.

You may sometimes hear classified information referred to as "National Security" information or "collateral" information.

"Collateral" refers to classified materials for which special requirements are not formally established.

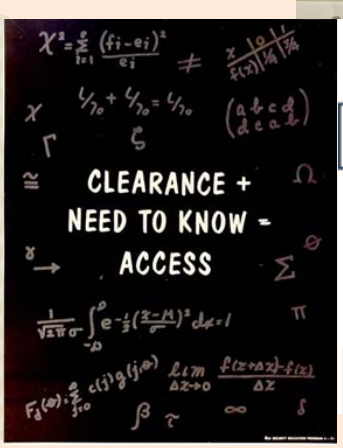
Rank, level, or position within the company does not equal a clearance or need-to-know.

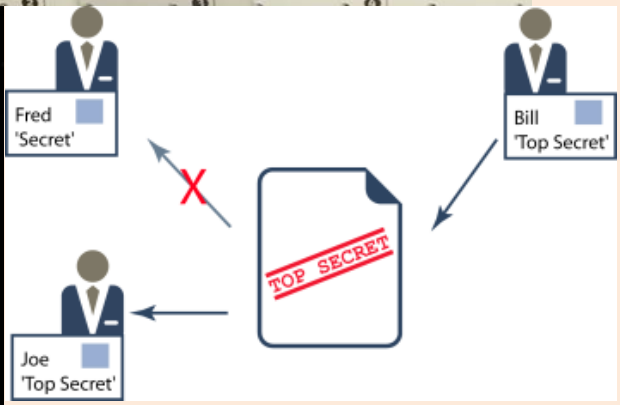
RELEASE OF INFORMATION

Prior to releasing information, the holder must ensure that the recipient of the information has both:

- Proper security clearance – Cleared individuals may access classified information at or below their clearance level
- Need-to-know – Each individual shall only be granted access to the specific classified information that is absolutely required to perform their job.

If you have a question about whether someone should have access to classified materials and information, ALWAYS contact your Facility Security Officer or Designated Security Representative.





PROCEDURES AND DUTIES (CONT)

HANDLING OF CLASSIFIED INFORMATION

Safeguarding

Some general safeguarding guidelines include:

- Never leave classified material unattended
- Secure classified material in a government-approved container or area
- Properly protect combinations that control access to classified materials and areas
- Understand how your facility secures classified materials and areas at the end of each day
- When transmitting classified information outside of an authorized facility, comply with all special requirements
- Take actions to prevent the loss or unauthorized disclosure of classified information; be mindful when holding classified discussions (such as hallways, cubicles, break rooms, etc.)
- Be aware of local policies or restrictions regarding cell phones, cameras, MP3 players, tablets, and any other personal electronic device entering classified areas
- Understand the various types of approved areas for classified operations including but not limited to closed and restricted areas
- Recognize that classified material comes in various forms (such as documents, hardware or assets, electronic media, communications or transmissions)

Reproduction

- Reproduction of classified material:
  - Should always be kept to a minimum
  - Should be performed only by authorized personnel familiar with the procedure
  - Should be performed only on authorized equipment

Transmission

- All classified materials coming in and out of a facility by mail, fax, or courier must be sent and received by the Facility Security Officer or Designated Security Representative.
- If you receive a classified package directly, notify your Facility Security Officer or Designated Security Representative IMMEDIATELY!

Retention / Disposition

- Contractors are authorized to retain classified material received or generated under a contract for two years following completion of the contract, unless other guidance is provided by the Government Contracting Authority (GCA).
- Classified material should only be retained for valid contract performance purposes and dispositioned when no longer needed.
- Destruction of classified information must be accomplished by authorized methods and personnel ONLY. Understand the destruction methods at your facility.

In case of emergency, follow all practical security measures for safeguarding classified material as the situation allows.

YOUR PERSONAL SAFETY COMES FIRST!

PROCEDURES AND DUTIES (CONT)

UNAUTHORIZED RELEASE OF CLASSIFIED INFORMATION

There are negative impacts associated with the unauthorized release of classified information. These impacts include but are not limited to:

- Damage to National Security
- Weakened integrity of classified information and technical advantage
- Damage to company reputation and customer relationships
- Potential negative impact on award fees
- Loss of classified contracts and/or exclusion from bidding
- Loss of personal security clearance and/or employment

DATA SPILLS

Data Spills, also known as data contaminations, are a form of unauthorized release of classified information. Data spills occur when classified information is either intentionally or unintentionally introduced to an unclassified or unaccredited information system. Improper handling of data is at the core of most data spills.

The best way to prevent a data spill is to focus on what you can control:

- Know where to find and how to use security classification guides for your program or project
- Properly handle and appropriately mark classified information
- If you receive or discover classified or potentially classified information on an unclassified information system, immediately contact your Facility Security Officer or Designated Security Representative for guidance. Do not forward, print, save, or delete the suspected information.

SECURITY INCIDENT REPORTING

The improper safeguarding, handling, reproduction, transmission, disposition, or disclosure of classified material is a reportable security incident.

If you commit or discover a potential security incident, immediately report the circumstances to your Facility Security Officer or Designated Security Representative and, if possible, ensure the material involved is properly safeguarded. When reporting an incident, be cognizant not to disclose classified information over unsecure means.

Security personnel will evaluate the circumstances and take actions as appropriate.

By adhering to security procedures, you ensure classified information is properly protected and contribute to the nation's security.

By properly protecting information, we meet our contractual obligations, enhance customer trust, help ensure University of Central Florida's continued ability to compete for new business opportunities, and maintain our reputation.

CLASSIFICATION OVERVIEW

Information becomes classified by a designated **Original Classification Authority** after it has been determined the information is owned, produced by or for, or controlled by the United States, and that unauthorized disclosure could result in damage to National Security.

When marking classified material (i.e. documents, media, or electronic files), the following must be included:

- The overall level of classification
- Title of the material
- Date created
- Name and address of the originating facility
- Identity of the classifier
- Period of time protection is required
- Any sources used to classify the information
- Any portions that contain classified information

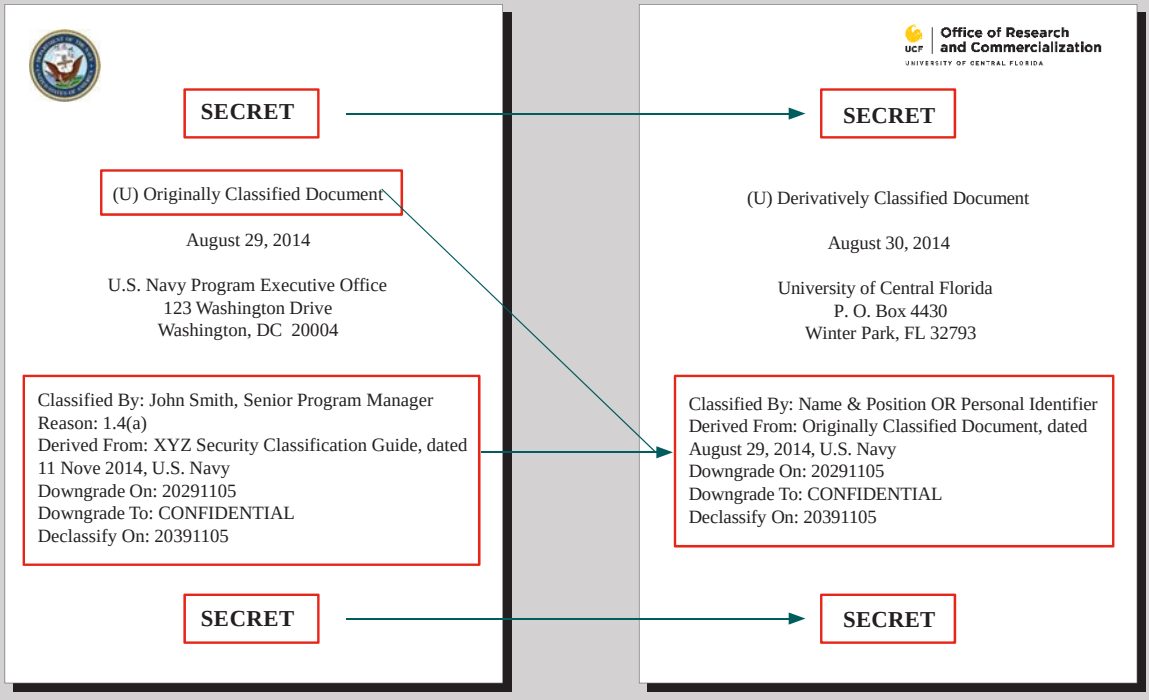
Classification markings may be identified from the following two places:

- Security Classification Guides (SCGs) or equivalent guideline authorized for your effort
- Existing properly marked source material authorized for use on your effort

Classification markings help facilitate proper safeguarding requirements and assist in the prevention of inadvertent release.

You may be required to perform **derivative classification decisions** in the course of your job responsibilities; if this is the case, you will receive additional training in greater detail.

Carrying forward these markings to newly-generated material is our responsibility as contractors, who make derivative classification decisions when we include existing classified information into new forms.



Classification markings and examples in this guide are for training purposes only.

INSIDER THREAT

What is an INSIDER THREAT?

It is a sad reality, but the United States has been betrayed by people holding positions of trust.

Arguably, “insiders” have caused more damage than trained, foreign professional intelligence officers working on behalf of their respective governments.

This information is intended to help (you) the contractors within the National Industrial Security Program recognize possible indications of espionage being committed by persons entrusted to protect this nation’s secrets.

Not every suspicious circumstance or behavior represents a spy in our midst, but every situation needs to be examined to determine whether our nation’s secrets are at risk.

DSS defines insider threat as: Acts of commission or omission by an insider who intentionally or unintentionally compromises or potentially compromises DoD’s ability to accomplish its mission. These acts include, but are not limited to, espionage, unauthorized disclosure of information, and any other activity resulting in the loss or degradation of departmental resources or capabilities.

How can YOU help?

You and your colleagues are the first line of defense against espionage. Help protect our national security by reporting any suspicious behavior that may be related to a potential compromise of classified information. Be aware of the actions of those around you and report suspicious behaviors.

INSIDER THREAT CASE STUDY

Economic Espionage:

Greg Chung, an engineer for a cleared defense contractor, stole over 250,000 documents containing trade secrets about the space shuttle, the Delta IV rocket, and the C-17 military cargo jet. He traveled to China under the guise of giving lectures while secretly meeting with Chinese agents.

In February 2010, he became the first person to be tried under the economic espionage provision of the Economic Espionage Act and was sentenced to over 15 years in prison.

Fort Hood Shooting:

In November 2009, an Army Major killed 13 people and wounded 29 others at Fort Hood, Texas. The shooting represents the worst shooting to ever take place at an American military base.

Six months prior to the shooting, the Major had been investigated for expressing extremist views, but was determined not to be a threat as the incident was related to his professional research.

Even before that, when he worked at Walter Reed Medical Center, he had concerned colleagues with his tendency towards conflict and comments concerning the American military presence in Iraq and Afghanistan.

At his court-martial in August 2013 he was convicted of 13 counts of premeditated murder, 32 counts of attempted murder, and unanimously recommended to be formally dismissed from the service and sentenced to death. He is incarcerated at the United States Disciplinary Barracks at Fort Leavenworth in Kansas awaiting execution while his case is reviewed by appellate courts.

COUNTERINTELLIGENCE

Counterintelligence is defined as information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage or sabotage; conducted for or on behalf of foreign powers, organizations, international terrorist groups or individuals.

What does that mean to you?

Counterintelligence is identifying intelligence threats to the University of Central Florida, other defense contractors, and our government customers, and developing strategies to mitigate those threats.

As a recently cleared employee with the University of Central Florida, it's important you understand these threats.

Intelligence threats can come from foreign intelligence services, foreign and/or domestic industry competitors, criminal, terrorist, and/or extreme activist organizations, and trusted insiders, also known as the insider threat.

Intelligence collection can come in a variety of different forms, including: elicitation, open source collection, electronic surveillance, cyber intrusions, social engineering, exploitation of social media, and formal recruitment.

Recruitment occurs when an employee collects information on behalf or at the direction of a foreign intelligence service. Formal recruitment is often the precursor to insider threat activity.

The insider threat is someone who has legitimate access to company or classified USG information and uses that access to steal information for their foreign intelligence service, on their behalf. Indicators of insider threat activity might include an apparent disgruntlement with employer or USG, disregard for security and IT procedures, outward expression of loyalties towards competitors or foreign nations, unreported foreign travel or foreign contacts, or a sudden shift in demeanor.

The ultimate goal of a foreign intelligence officer is successful recruitment of an employee who can act as an insider on their behalf. As a University of Central Florida employee and a member of the cleared community, you are an elevated target for recruitment and intelligence collection by those that seek access to classified information and classified information systems.

You are also in the best position to observe behaviors suggesting concerns of an insider threat in the workplace. Employee should contact their Facility Security Officer or Designated Security Representative immediately if they have concerns they've been involved in a recruitment attempt or other intelligence collection attempts, or if they have any concerns of potential insider threat activity in the workplace.

Foreign Intelligence Services | **Foreign and/or Domestic Industry Competitors** | **Criminal, Terrorist, and/or Extreme Activist Organizations** | **Trusted Insiders**

CONCLUSION

This initial security training provided you with information on:

- Your reporting requirements
- The security duties and procedures applicable to your job
- The Security Classification System
- Counterintelligence, the insider threat, and defensive security practices to mitigate these threats

Remember that each area/ facility supports unique contracts and may implement requirements in slightly different ways. To be successful in your new role as a cleared University of Central Florida employee, it is imperative that you work closely with your Facility Security Officer or Designated Security Representative regarding the content reviewed in this initial security training and any additional area/facility specific requirements.

YOUR SECURITY CLEARANCE ELIGIBILITY IS A CONTINUING RESPONSIBILITY!

Now that you have received your security clearance, you play an integral part in ensuring the success of University of Central Florida Security Program and our National Security. The nature of your new responsibilities relates directly to our customers.

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 your Facility Security Officer or Designated Security Representative.

Completing the Non-Disclosure Agreement (NDA/Standard Form 312)

Now that you have completed this training, please schedule an appointment with UCF's Facility Security Officer or Designated Security Representative to complete the required Classified Information Non-Disclosure Agreement also known as the Standard Form (SF) 312.

Before being granted access to classified information, you must first sign a Non-Disclosure Agreement or NDA. The NDA is a **legal** and **binding** contract between you and the U.S. Government whereby you agree to protect any and all classified national security information to which you will have access.

Be advised that the NDA is binding for LIFE! A Life-Long Commitment!

GLOSSARY

Collateral – All National Security information classified Confidential, Top Secret or Secret under the provisions of an executive order for which special community systems of compartmentation (e.g., non-Special Compartmented Information (non-SCI)) are not formally established

Confidential – A level of classification that is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause damage to National Security

Courier – An individual who has been briefed and meets the requirements to transport classified materials

Derivative classification decisions – The 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 applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

DoD – Department of Defense

DSS – Defense Security Service

Information System (IS) – An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Insider – Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.

Insider Threat – The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

GCA – Government Contracting Authority, which provides guidance to contactors

Need-to-know – must be in place along with a security clearance to be granted access to specific classified information required to perform a job

NISPOM – National Industrial Security Program Operating Manual

Secret – A level of classification that is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause serious damage to National Security

Security clearance - An administrative authorization for access to National Security information up to a stated classification level (Top Secret, Secret, Confidential).
NOTE: A security clearance does not, by itself, allow access to controlled access programs

Top Secret – A level of classification that is assigned when the unauthorized disclosure of information or material could reasonably be expected to cause exceptionally grave damage to National Security

USG – United States government

An extensive list of security terms can be found at the Defense Security Service website.