- Threat Awareness
- Defensive Security
- Security Classification
- Reporting Obligations and Requirements
- Security Procedures and Duties Applicable to Your Job
- SF 312, Nondisclosure Agreement
THREAT AWARENESS

- **What are we protecting?**
  - **Classified Information**
    - US Government classified material (*Top Secret, Secret, Confidential*)
  - **Company Proprietary Information**
    - Also known as intellectual property. This category includes knowledge and information created and maintained within the company for the sole financial benefit of the company.
  - **Company Private Information**
    - Also known as company sensitive information. This category includes all other internal company information such as employee data, contract bidding information, and so on.
  - **Contract-Specific Information**
    - Information that pertains directly to a specific contract. This information is restricted to personnel directly involved with a specific contract.

- **BOTTOM LINE:** Safeguard all information
• **How are we vulnerable or susceptible?**
  - Face-to-Face Contacts
  - Telephone Contacts
  - Written Contacts
  - Public Information on Privately Held Companies
  - **Local Sources**: Government & Non-Governmental
    - **State Gov’t**: General Business Interests/Specific Industries
    - **Fed. Gov’t**: General Business Interests/Specific Industries
    - **Numerous other sources**: Courts, Credit Reporting Agencies, Manufacturers, Suppliers, Distributors, Publishers, Trade & Professional Associations

• **BOTTOM LINE**: Immediately report suspicious activity to FSO
• **How can we protect ourselves and our information?**
  
  - For every vulnerability, there are protective measures
  - Some common sense precautions include:
    - Avoid unnecessary discussions of company business
    - Avoid public discussions of company business
    - Verify identity of person seeking information
    - Establish person’s Need-To-Know **BEFORE** releasing information
    - Screen your documents **BEFORE** discarding
    - Adequately destroy company-sensitive information when discarding
    - Computer security (Use boot-up, internal & screensaver passwords)
    - Use removable hard drives and floppy disks for sensitive information

• **BOTTOM LINE**: When in doubt, don’t release information
- Birth of the Electronic Age has necessitated new Laws
  - Uniform Trade Secrets Act
  - Economic Espionage and Protection of Proprietary Economic Information Act of 1995
  - Industrial Espionage Act of 1996
  - Economic Security Act of 1996

- Electronic Age and necessitated new Defensive Technology
  - Cyberspace Law School
  - Firewalls
  - Infinite Virus Scans
  - Data Security Systems

**BOTTOM LINE:** Being defensive means being proactive
SECURITY CLASSIFICATION

- **CONFIDENTIAL**
  - The designation that shall be applied to information or material the unauthorized disclosure of which could be expected to cause **DAMAGE** to the National Security

- **SECRET**
  - The designation that shall be applied to information or material the unauthorized disclosure of which could be expected to cause **SERIOUS DAMAGE** to National Security

- **TOP SECRET**
  - The designation that shall be applied to information or material the unauthorized disclosure of which could be expected to cause **EXCEPTIONALLY GRAVE DAMAGE** to the National Security

- **BOTTOM LINE**: Know and follow all proper procedures for the level of classified information involved
Employee Reporting Requirements

- The NISPOM relies on individual trust and responsibility
- Contractors are required to report certain events impacting:
  - Status of Facility Clearance
  - Status of Personal Clearance
  - Proper Safeguarding of Classified Information
  - Possible Loss or Compromise of Classified Information

Situations to Report

- Suspicious Contacts
- Adverse Information
- Loss or Compromise
- Change in Personal Status
- Other Reporting Requirements

BOTTOM LINE: When in doubt, report it
• **Suspicious Contacts**
  
  - Report *any* suspicious behavior or occurrences, including:
    - Contacts with known or suspected intelligence officers from any country
    - Contacts suggesting an employee may be target of an attempted exploitation by a foreign intelligence service
  
  - More specifically, employees *must* report any of the following events:
    - Any efforts, by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified or sensitive unclassified information
    - Any efforts, by any individual, regardless of nationality, to compromise a cleared employee
    - Any contact with a cleared employee with a known or suspected intelligence officer from any country
    - Any contact which suggests an employee may be the target of an attempted exploitation by the intelligence services of another country

• **BOTTOM LINE**: Report any of these situations to the FSO
**Adverse Information**

- Adverse information, as a general rule, is any information that reflects adversely on the integrity or character of an employee, and suggests that his/her ability to safeguard classified information may be impaired.

- Reported Adverse Information Treated as Confidential
  - Subject need Never Know the Originator

- Examples of Adverse Information (not an all-inclusive list):
  - Criminal activities
  - Financial Concerns (Unexplained Affluence or Sudden Excessive Debt)
  - Emotional or Mental Disorders (i.e., Sudden Depression, etc.)
  - Excessive Use of Alcoholic Beverages
  - Use of Illegal/Controlled Substances (i.e., marijuana, cocaine, etc.)
  - Mishandling of Classified or Sensitive Information
  - Sudden Change in Lifestyle

**BOTTOM LINE:** Report possible adverse information to the FSO
• **Loss or Compromise**
  - Employees are required to report any loss, compromise or suspected compromise of classified information, foreign or domestic, to the appropriate security office.
  - Reporting provides employees an opportunity to extricate themselves from a compromising situation and enhances the protection of national security information.
  - Covering up a known security infraction undermines the security education process, and jeopardizes the relationship of mutual trust between the contractor and the Cognizant Security Agency.
  - Security Violations may include such acts as (not an all-inclusive list):
    - Misplacing
    - Losing
    - Improperly Storing
    - Improperly Transmitting
    - Leaving Classified Unattended
REPORTING OBLIGATIONS AND REQUIREMENTS

- **Change in Personal Status**
  - Contractors must submit a report to CSA for the following information:
    - Death of an employee
    - Termination of Employment
    - Change in an employee’s Marital Status
    - Change in an employee’s Citizenship
    - Possibility of future access to classified has been reasonable foreclosed
    - Becoming a Representative of a Foreign Interest (RFI); or if your status is an RFI is materially changed
  - Cleared employees are required to report changes in personal status
  - Examples of Adverse Information (not an all-inclusive list):
    - Change in Personal Information (i.e., Name, Address, etc.)
    - Lawsuits
    - Arrests and Convictions
    - Foreign Travel
    - Foreign Associations

- **BOTTOM LINE**: Report any changes in personal status to the FSO
• **Other Reporting Requirements**

  - In addition to the previously mentioned reporting requirements, employees are required to report any act of sabotage or possible sabotage, espionage or attempted espionage, and any subversive or suspicious activity.
  - Employees are encouraged to report any of the following activities:
    - Attempts to solicit classified information
    - Unauthorized persons on company property
    - Citizenship by naturalization
    - Employees are not desiring to perform on classified work
      - Evidence that an employee no longer wishes to be processed for a clearance or to continue an existing clearance
    - Disclosure of classified information to an unauthorized person
    - Any other condition which would qualify as a security violation, or which common sense would dictate as worth reporting

• **BOTTOM LINE:** Report any of these situations to the FSO
REPORTING OBLIGATIONS AND REQUIREMENTS

- **Key Reporting Information**
  - Facility Security Officer:
    - Mike Seidl
    - (719) 599-1381
  - DOD Hotline
    - Defense Hotline
    - The Pentagon
    - Washington, DC 20301-1900
    - (800) 424-9098
    - (703) 693-5080
General Security Procedures

- Know Your Work Area
  - Be familiar with your immediate office area, especially your desk area
  - Be familiar with all entrances/exits and windows
  - Be familiar with all employees having unescorted access into your area

- Practice Basic Security Techniques
  - CHECK your immediate work area for anything suspicious when you arrive for duty every day; and do the same when you depart for the day
  - BE AWARE of any unusual or suspicious behavior from co-workers
  - CLOSELY GUARD classified and company-sensitive materials/information
  - INSTALL password-activated boot-up and screensavers to protect data
  - LISTEN carefully during phone calls for unusual background noises
  - READ E-Mail Sender Addresses and Subject Lines before opening
  - Diligently maintain and USE an office end-of-day security checklist

BOTTOM LINE: Cautious is good; better safe than sorry
SF 312, CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

- NISPOM, Paragraph 3-105 states requirements:
  - This document is an agreement between the United States and an individual who is cleared for classified information
  - Individual must read and sign an SF 312 form BEFORE being given access to classified information
  - Security representative should also verbally communicate to individual what the agreement represents
  - SF 312 is essentially a lifetime contract between the individual and the U.S. Government, in which the employee agrees to protect U.S. classified information from unauthorized disclosure
  - If an individual refuses to execute the SF 312, the contractor will deny the individual access to classified information and submit a report to the Cognizant Security Agency
SUMMARY

- Threat Awareness
- Defensive Security
- Security Classification
- Reporting Obligations and Requirements
- Security Procedures and Duties Applicable to Your Job
- SF 312, Nondisclosure Agreement

THAT'S ALL FOLKS. GO FORTH AND KEEP THOSE SECRETS SAFE.