INITIAL SECURITY BRIEFING
Topics:

- Physical Security
- Personnel Security
- Information Security
- Threat Awareness
- Defensive Security
- Cybersecurity
- Public Release of Information
- Operations Security
- Policies
Understand National and DoD security policies to counter threats.

Identify threats to classified and unclassified government assets including, but not limited to:

- Insider
- Criminal and Terrorist Activities
- Foreign Intelligence Entities
- Foreign Governments

The only thing between our adversaries and classified/proprietary information is you and the diligent performance of YOUR SECURITY responsibilities.
PERSONNEL

Know your UA security officer:

Keith A. Corson
University of Arizona
Facility Security Officer
(520) 626-5865
kcorson@email.arizona.edu

Your sponsor’s cleared facility will also have a local security officer with information specific to that location
PHYSICAL SECURITY
PHYSICAL SECURITY

Includes, but is not limited to:

- Antiterrorism
- Employee and visitor access controls
- Badging
- Intrusion Detection Systems
- Guards/patrols
- Prohibited items
- Entry/exit inspections
- Escorting

- Training will be provided to you at the specific site where you access classified material
- You are required to follow the rules of your host site
- No classified material or information of any kind is allowed on the UA campus or a UA facility
Position sensitivity and/or duties determine level of clearance and access

Clearance levels

- Top Secret, Secret, or Confidential

UA is a non-possessing facility cleared to the Secret level. UA employees may only be cleared to the Secret level. There is no approved location on campus or at any UA facility to hold or access classified information or conduct classified research.

All access to classified information and classified research conducted must take place at the sponsor’s secure facility.
PERSONNEL SECURITY | BACKGROUND INVESTIGATION

- **Includes investigations for:**
  - DoD Civilians
  - Military
  - Contractors

- **Conducted to determine suitability for granting a security clearance**
  - Single Scope Background Investigation (SSBI)
  - Access National Agency Check and Inquires (ANACI)
  - National Agency Check with Law and Credit (NACLC)

- **Subject to continuous evaluation**
  - SSBI-Periodic Reinvestigation (SSBI-PR)
  - Phased Periodic Reinvestigation (PPR)
  - NACLC
**Need-to-Know** is generally based on a contractual relationship between the contractors. The responsibility for determining need-to-know rests with the individual who will disclose classified information.

Having a clearance does not automatically mean you can have access to classified information – there must also be a need-to-know the classified information you will receive.
• Coordinate access debriefing during out-processing
• When you leave your job or it is determined you no longer require access to classified material, you will be debriefed
• The security office of your sponsor’s cleared facility will also provide you with specific instructions
• **Changes to:**
  • Name
  • Marital Status
  • Citizenship

• **Adverse information**
  • Based on facts *NOT* rumors
  • Self or co-worker
    
    Includes but not limited to:
    - Criminal activities
    - Alcohol or drug related incidents
    - Financial difficulties
• **Loss, compromise, or suspected compromise of classified information**
  - Secure information immediately
  - Report immediately to security or supervisor
  - Contact host site security immediately

• **Foreign contacts**
  - Continuous contact with foreign nationals
    - Includes, but is not limited to:
      - Cohabitation
      - Marriage
  - Suspicious contacts with or by foreign nationals
  - Member of immediate family or spouse’s immediate family is a citizen of a foreign country
• **Foreign Travel**
  • Advise UA FSO prior to any planned foreign travel, whether personal or work-related. Also, a foreign travel de-briefing must take place upon your return.
  • Your sponsor’s FSO may also inform you of actions they require

• **Other employment or service**
  • Foreign government, national, organization or entity, or a representative of any foreign interest (paid or unpaid)

• **Lost or stolen badges**
  • Follow the process described by the security office of your sponsor’s cleared facility
Suspicious Contacts

Suspicious contact is an attempt by foreign entities or competitors to collect information. Reporting of suspicious contacts makes it possible for the Government and private industry to monitor foreign entities/competitors, provide warnings, and detect/neutralize foreign threats.
Potential Espionage Indicators Exhibited by Others

- Unexplained affluence
- Keeping unusual work hours
- Divided loyalty or allegiance to the U.S.
- Willfully disregarding security procedures
- Unreported foreign contact and travel
- Pattern of lying
- Attempts to enlist others in illegal or questionable activity
- Verbal or physical threats
- Inquiring about operations/projects where no legitimate need to know exists
- Unauthorized removal of classified information
- Fraud/Waste/Abuse of government credit cards
The best way for you to help your security program is to participate in your security program. A significant part of the security program is reporting. In addition to reporting adverse information and suspicious activities, you should make reports to UA’s FSO or your sponsor’s security office on the following:

• Non-compliance with published security policies and procedures
• Blatant disregard for security policies and procedures
• Unauthorized removal of classified or proprietary information from work
• Falsification of locations visited during travel
• Sudden unexplained affluence
You should also make reports on the following:

- Falsifying destruction records
- Careless destruction of proprietary information
- Frequently working after hours or at unusual times
- Requests for access to information that is not related to assigned tasks
- Inquiries to other employees about their work not related to normal tasks
- Excessive use of photocopying equipment
- Repeated and continued patterns of performance deterioration
INFORMATION 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

You are always required to follow the guidelines provided by the security office of your sponsor’s cleared facility.

At a UA facility, please contact Keith Corson, (520)626-5865; or kcorson@email.arizona.edu
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:
  - For Official Use Only (FOUO)
  - Law Enforcement Sensitive (LES)
  - Sensitive But Unclassified (SBU)
  - Export Controlled Information (ECI)
INFORMATION SECURITY | CLASSIFICATION LEVELS

**TOP SECRET** Exceptionally Grave Damage to the National Security

**SECRET** Serious Damage to the National Security

**CONFIDENTIAL** Damage to the National Security
Includes, but is not limited to:

- Machinery
- Documents
- Emails
- Models
- Faxes
- Photographs
- Reproductions
- Storage media
- Working papers
- Sketches
- Maps
 Appropriately marked to alert recipients of the information’s classification

TOP SECRET (TS)
SECRET (S)
CONFIDENTIAL (C)
How Is Information Classified?

- **Original Classification**
  - Only specific positions within the U.S. Government can originally classify information

- **Derivative Classification**
  - All cleared and trained DoD and contractor personnel can be derivative classifiers

  Derivative Classification: Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
What Information Can Be Classified?

Only Information that falls under one or more categories of section 1.4 of Executive Order 13526 may be eligible to be classified:

a) military plans, weapons systems, or operations
b) foreign government information
c) intelligence activities (including covert action), intelligence sources, methods, or cryptology
d) foreign relations or foreign activities of the United States, including confidential sources
e) scientific, technological, or economic matters relating to the national security
f) United States Government programs for safeguarding nuclear materials or facilities
g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
h) the development, production, or use of weapons of mass destruction
Information cannot be classified to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of the national security
- Classify basic scientific research information not clearly related to national security
Classification Challenges

• You have a responsibility to report information that you believe is improperly or unnecessarily classified.

• Contact your security official for additional guidance for submitting a classification challenge.
INFORMATION SECURITY

Safeguarding 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 respect and understand the markings and the downgrade/declassification instructions on classified material
- Must receive appropriate training prior to performing derivative classification duties and refresher training every two years thereafter
- Discuss or send via secure communications
- Process on approved equipment
- Destroy by approved methods
- Discuss in an area authorized for classified discussion
INFORMATION SECURITY

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
- For additional information contact:
  - Security Official at your sponsor’s cleared facility, or
  - Keith Corson, UA FSO (520) 626-5865, kcorson@email.arizona.edu
Sanctions

- Sanctions may include, but are not limited to:
  - Warning
  - Reprimand
  - Loss or denial of classified access
  - Suspension without pay
  - Removal from employment
  - Discharge from military service
  - Criminal prosecution
THREAT AWARENESS
The Threat: Foreign Intelligence Threat

- **Gathering of information by intelligence agents**
  - Intelligence officers, those individuals working for government intelligence services, are trained to serve their country by gathering information.
  - Spies, on the other hand, betray their country by espionage.
  - Targets are shifting away from the classified military information sought in the old Cold War days toward basic research and development processes.
  - Any information or process – whether classified, unclassified or proprietary – that leads to cutting-edge technology is plainly in demand.
  - More often now, theft of high-technology information, classified or not.
  - Preventing this kind of betrayal is the ultimate goal of the entire U.S. personnel security system.
The Threat: Foreign Intelligence Threat

• Although the threat is global, the predominant threats come from the following regions:
  • Europe
  • Eurasia
  • Asia
  • Middle East & Northern Africa
  • South America

• Art of spying is not a game
  • The U.S. can be weakened by the theft of its vital knowledge, and its enemies can be strengthened by the acquisition of that knowledge, whether it is classified or unclassified
The Threat: Foreign Intelligence Threat

- **Objective:**
  - Wholesale collection of data
  - Obtain government documents

- **Techniques**
  - Unsolicited requests for Scientific and Technologic Information
    - Any request received from a known or unknown source which concerns classified, sensitive, or export-controlled information
Indicators of Being a Target

- **Be wary of:**
  - Requests from foreign country internet addresses
  - Requests from unknown sender/requestor
  - Technology request is for classified or export controlled information
  - Request for information from foreign government or foreign government program
  - Use of acronyms specific to the program or area of research
  - Requests disguised as ‘marketing surveys’
  - Inappropriate conduct during foreign visits
  - Strangers making intensive effort at forming friendships

- **Do not respond to a suspicious request**
  - Inform sponsor facility security office or Keith Corson, UA FSO
    (520) 626-5865, kcorson@email.arizona.edu
DEFENSIVE SECURITY
Beware of Possible Risks During Foreign Travel or During Contact with Foreign Persons

- Cleared contractor personnel are considered prime targets of Foreign Intelligence Services and terrorist groups
- Elicitation is the art and science of engaging someone in simple, “innocent” conversation for the purpose of getting the targeted individual to speak openly and more in-depth
- Appealing to the American belief in freedom of speech and the free exchange of information
- May include coercion and blackmail

- Do not reference your access to classified information
- Do not leave valuables or important papers lying around your hotel room
- Do not travel with anything more than you can afford to lose
Contact With Representatives of Foreign Countries

- You are the target!
- Foreign countries are targeting newly developed, critical technologies (usually unclassified) having direct military application
- Foreign competitors view industrial espionage as a legitimate practice and will exploit vulnerabilities when they see them
- Do not rely on appearance or voice accent alone. Foreign competitors work hard to look, sound, and act like you
Attending an international event, either in U.S. or abroad

- International events on high-tech topics attract many foreign scientists and engineers, providing foreign intelligence collectors with a concentrated group of specialists on a certain topic
- Opportunities for contact with representatives of foreign countries have increased. Be vigilant when participating in the following:
  - Hosting a visit
  - Attending:
    - Conventions
    - Seminars
    - Conferences
    - Symposiums
- Be wary if your movement/lodging is pre-arranged during international visits for these activities or if your agenda changes
- Report suspected incidents to sponsor security office or Keith Corson, UA FSO (520) 626-5865, kcorson@email.arizona.edu
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 and tablets
- Electronic communications systems/services
- Personal Digital Assistant (PDA) (i.e. BlackBerry)
- Smartphones
Responsibilities

- Comply with password policy directives and protect passwords from unauthorized disclosure

- Contact your sponsor’s facility IT or security office for additional guidance

- At UA, contact University Information Technology Services (520) 626-8324
PUBLIC RELEASE OF INFORMATION
• Release of government information must be approved by the Public Affairs Office (PAO)

• Do not discuss classified or sensitive information with the media; refer inquiries to your local PAO

• Contact your sponsor’s secured facility FSO or PAO for additional information

• At the UA campus, contact Keith Corson (520) 626-5865
Operations Security (OPSEC) is a systematic process that is used to mitigate vulnerabilities and protect sensitive, critical, or classified information.

Security Procedures Specific to Your Sponsor’s Cleared Facility
- Contact your sponsor’s security manager/office for additional guidance.

At the UA campus, contact Keith Corson (520) 626-5865
- No classified research or materials can take place or be held at a UA facility.
- All export controlled research/technology at UA must be covered by a Technology Control Plan. For more information: [www.orcr.arizona.edu/ec](http://www.orcr.arizona.edu/ec)

For Information Technology Security information at UA, contact University Information Technology Services (520) 626-8324.
Reference Security Policies and Regulations (not all inclusive):

- Executive Order 13526 - Classified National Security Information
- Executive Order 12968 - Access to Classified Information
- DoDD 5205.02E, DoD OPSEC Program
- DoDI 2000.12, DoD Antiterrorism (AT) Program
- DoDI 8500.01, Cybersecurity
- DoDM 5200.01, Vol. 1-4, DoD Information Security Program
- DoD 5200.2-R, DoD Personnel Security Program
- DoD 5200.08-R, DoD Physical Security Program
QUESTIONS

Contact List

The FSO or Security Office of your sponsor’s cleared facility

or

Keith A. Corson
University of Arizona
Facility Security Officer
(520) 626-5865