KeplerResearch

Initial Orientation and Awareness Training

Initial & Annual Orientation Training is required per DoDM 5200.01, Vol. 3, Enclosure 5.

This training provides basic security knowledge to recognize and respond to threats to National Security Information.

KeplerResearch

YOUR SECURITY POINTS OF CONTACT

Margie Heminger (FSO)

James Wilson (Alt FSO)

Barbara Russell (Alt FSO)

13663 Office Place

Suite 202

Woodbridge, VA 22192

Phone: 703-465-4035

KeplerResearch

CLASSIFIED DOCUMENTS CANNOT BE BROUGHT TO KEPLER'S OFFICE.

ALL CLASSIFIED VIEWING & STORAGE MUST BE DONE AT CLIENT SITES.

KeplerResearch

OUR SECURITY PROGRAM VISION

- **It is the policy of Kepler Research to develop, implement and maintain a viable Security Training Program which consistent with:**
  - -Kepler Research Policies
  - -Public Law
  - -National Security Policies
  - -Applicable Executive Orders
  - -DoD Directives & Regulations

- **Your Kepler Research Security Mangers develop, manage, and implement programs that protect the U.S. Government's vital information.**

AGENDA

- Personnel Security Clearance Process
- Information Security Program
- Pre-Publication Process
- Physical Security Program
- Operations Security (OPSEC) Program
- Understand the requirements for reporting foreign travel

Personnel Security

The Personnel Security Program: *This program provides security policies and procedures; establishes standards, criteria, and guidelines for personnel security determinations and overall program management responsibilities.*

Position Designations

Special-sensitive: Access to Sensitive Compartmented Information (SCI)/Top Secret (TS) or Special Access Program (SAP). Potential for inestimable damage to National Security.

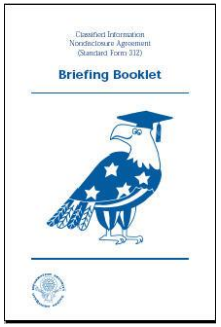
Critical-sensitive: Access to Top Secret (TS). Potential for exceptionally grave damage to National Security.

Noncritical-Sensitive: Access to Secret or Confidential. Potential for significant or serious damage to National Security.

Non-sensitive: No Clearance or other sensitive

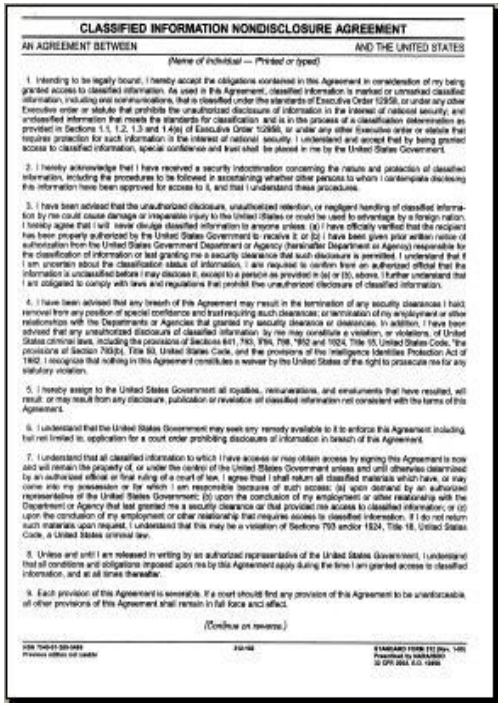
Personnel Security

SF312 – Agreement between U.S. Gov't and individual to protect classified data in their trust


Classified Information Nondisclosure Agreement (Standard Form 312)

Briefing Booklet

All employees must review & sign PRIOR to access to U.S. Gov't classified information.


CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual — Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

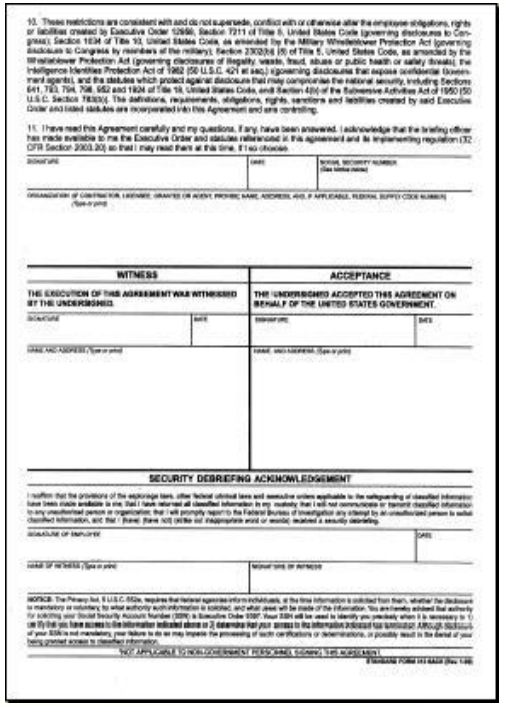
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)


10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosures to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE | DATE | SOCIAL SECURITY NUMBER (See notice below)

ORGANIZATION OF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER (Type or print)

WITNESS	ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.	THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.
SIGNATURE / DATE	SIGNATURE / DATE
NAME AND ADDRESS (Type or print)	NAME AND ADDRESS (Type or print)

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I [have] [have not] (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE / DATE

NAME OF WITNESS (Type or print) / SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

KeplerResearch

Personnel Security Clearance Process

Investigation

Adjudication

Periodic Reinvestigation

Self-Reporting

Personnel Security Investigation

Investigation

- New Federal Investigative Standards (FIS)
- Uses a five-tiered approach

Five-Tiered Investigative Model

Adjudications

- DoD Consolidated Adjudications Facility (DoD CAF) is the primary authority for making security clearance eligibility determinations
- Uses whole person concept
- Uses 13 Adjudicative Guidelines

SCURITY CHANGES

- DCSA is transitioning from Defense Information System for Security (DISS) to National Background Investigation Services (NBIS) System

- The National Background Investigation Services (NBIS) is the federal government's one-stop-shop IT system for end-to-end personnel vetting — from initiation and application to background investigation, adjudication, and continuous vetting. NBIS is one consolidated system designed to deliver robust data protection, enhance customer experience, and better integrate data across the enterprise.

- Secret & Confidential access now called Tier 3
- Top Secret now called Tier 5
- DCSA could entered individual into Continuous Evaluation (CE) program instead of performing Periodic Reinvestigation (PR)
- Pentagon (Defense Counterintelligence & Security Agency) in charge of background investigations for security clearances instead of Office of Personnel Management

Periodic Reinvestigation

Tier 3R: Secret and Confidential

Tier 3 Reinvestigations will continue to be conducted every 10 ten (10) years.

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

Reinvestigations have been extended from five (5) years to six (6) years with DNI endorsement.

After receiving PR, DSS will decide if CE is appropriate

See DoD Memorandum "Extension of Periodic Reinvestigation Timelines to Address the Backlog Investigation Backlog" <http://www.cdse.edu/documents/toolkits-psa/extension.pdf>

Self Reporting

Report changes in:

Status: Marriage, co-habitation, addition of new family member

Adverse Information (See DCSA Self-Reporting Factsheet):

- Criminal activity (domestic violence, issuance of restraining order)
- DUI/DWI
- Traffic tickets over $300
- Excessive indebtedness, financial difficulties, bankruptcy
- Use of illegal drugs

Foreign Contacts: Close or continuing association with foreign nationals

Reporting does not automatically result in revocation of eligibility, so don't be afraid to report!

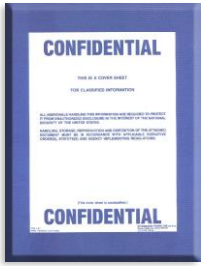
The Information Security Program is a system of policies, procedures, and requirements established to protect classified and controlled unclassified information (CUI) that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to National Security.

(Kepler will provide additional CUI policies and procedures)

Information Security
Levels of Classified Information

Top Secret: Could cause exceptionally grave damage to national security (SF703)

Secret: Could cause serious damage to national security (SF704)



Confidential: Could cause damage to national security (SF705)

ORIGINAL CLASSIFICATION: *The initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.*

- Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials to whom they delegate this authority in writing.
- Delegation of OCA shall be limited to the minimum number of officials required for effective operation of the Department of Defense.
- The authority shall be delegated to, and retained by, only those officials who have a demonstrable and continuing need to exercise it.

Executive Order (EO) 13526

Classified National Security Information

Executive Branch Information

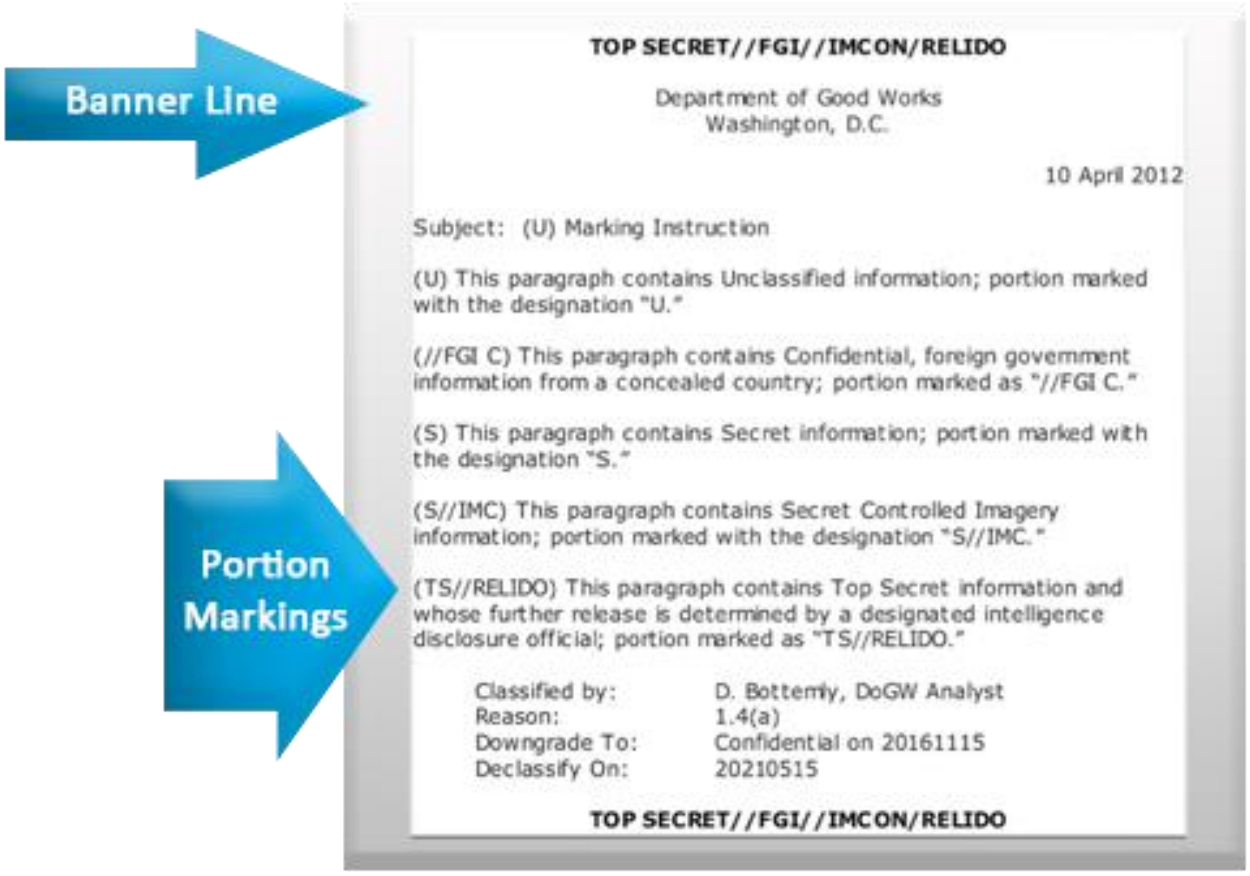
DERIVATIVE CLASSIFICATION: *Defined as incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.*

Derivative Classification Requirements

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

Information Security Marking Syntax

UNCLASSIFIED



Classification Markings are for Training Purposes Only

UNCLASSIFIED

Slide Presentations

- Mark title slide with overall marking and classification authority block
- Mark successive slides with overall classification and portion markings for bullets
- Mark slide graphics with overall classification

Follow Client Site Guidance

Working Papers

- Mark with highest classification of any information contained in the document
- Date and annotate as “Working Papers”
- Destroy when no longer needed or remark within 180 days

Reproduction Guidelines

- Use equipment approved at the appropriate level
- Ensure copies are subject to same controls as original
- Limit reproduction to what is mission essential
- Comply with reproduction limitations
- Facilitate oversight and control

Follow Client Site Guidance

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

Do Not

Follow Client Site Guidance

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

CUI: *Unauthorized disclosure could cause foreseeable harm.*

Examples of CUI

- Investigation documents
- Inspection reports
- Agency budgetary information
- Procurement bids/proposals
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial Information
- Personal or payroll information
- Information protected under Privacy Act of 1974

Information Security Safeguarding

Safeguard Classified Information

- GSA approved container
- Vaults
- Secure rooms
- Secure telephone
- Maintain control, never leave unattended
- Do not talk around using codes or hints
- Do not divulge to unauthorized persons

Safeguard CUI

- Properly Mark
- Locked cabinets
- *Rooms with locked outer office doors*
- *Key or cipher locked rooms*

Follow Client Site Guidance

Storage Containers

GSA Approved Containers: *Required for storing all classified materials*

Standard forms to be completed:

Follow Client Site Guidance

SF700: Security Container Information

- ✓ Record combinations to security containers, secure rooms, and controlled area doors

SF701: Activity Security Checklist

- ✓ Must be completed after all areas have been secured

SF702: Security Container Checklist

- ✓ Record date and time when opening or closing security container

Checklist for Mailing Classified Information

- Cover sheet required; opaque envelope
- Mark highest classification level
- Wrap and tape envelope
- Address properly
- Complete a document receipt
- Mitigate tampering

Follow Client Site Guidance

Transmit/Transport Top Secret/SCI

- Direct contact between cleared U.S. personnel
- Protected facsimile, message, voice [secure telephone equipment (STE)]
- Appropriately cleared courier

Do Not Send Via

- U.S. Postal Service
- *Overnight Express (FedEx)*

Follow Client Site Guidance

Transmit/Transport Secret

Follow Client Site Guidance

- U.S. Postal Service registered mail or priority mail express within U.S. and Puerto Rico
    - Check “Signature is Required” box
- U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service outside the U.S. and territories
    - Information may not pass out of U.S. citizen control
- Commercial delivery for urgent, overnight delivery only
- Open incoming packages immediately and secure

Transmit/Transport Confidential

Follow Client Site Guidance

- U.S. Postal Service certified mail to DoD contracting companies or non-DoD agencies
- U.S. Postal Service first class mail between DoD components in the U.S. and its territories
    - Outer envelope marked “Return Service Requested”

DO NOT use external or street side mail collection boxes

Transmit/Transport CUI

- U.S. Postal Service certified mail, parcel post, or fourth class mail
- Approved secure communications systems
- Facsimile if appropriate protection is available at receiving location

Follow Client Site Guidance

Hand Carry Requirements

- Prepare inventory
- Double wrap material
- Keep under constant control
- Deliver to authorized person
- Receive courier briefing
- Carry courier card
- Carry courier letter if transporting via commercial air

Follow Client Site Guidance

Information Security Destruction

Destruction of Classified Material

- NSA approved crosscut shredder
- Burning
- Wet pulping
- Mutilation
- Chemical decomposition
- Pulverizing

Destruction of CUI

- Same methods as classified
- Other methods that would not allow recognition or reconstruction

Follow Client Site Guidance

Security Incident: *Categorized as infraction or violation*

Infraction

- No loss or compromise

Violation

- Loss – material cannot be accounted for or physically located
- Compromise– material disclosed to an unauthorized person
- NDCI - occurs when data is placed on an IT system with insufficient controls at the required classification level

Report infractions and violations immediately to your security officer (Kepler & Client Site)

Sanctions

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

- Disclose classified or CUI to unauthorized persons
- Classify information in violation of DoD regulations

Sanctions include:

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

Classified Information in the Public Media

- Do not confirm or deny
- Do not respond to questions about programs or projects

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

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

Materials subject to pre-publication review include:

- Books, manuscript, or articles sent to the publisher, editor, movie producer, or game purveyor, or their respective support staffs
- Speech, briefing, article, or content that will be publically disseminated
- Information released to the public, even through Congress or the courts

See DoDI 5230.29 Security and Policy Review of DoD Information for Public Release

Working with Gov't Employees & Other Contractors

- Contractors & Gov't Employees may or may not be cleared
  - Verify through a valid visit authorization and/or DD Form 254, Department of Defense Contract Security Classification Specification
  - Cleared under National Industrial Security Program (NISP)
  - Follow requirements of DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)
  - Required to comply with your organization's security program

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

Physical Security

***Physical Security**: Concerned with active and passive measures to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity.*

Physical Security Countermeasures

- Barriers/Fencing: establish boundaries and deter individuals
- Intrusion Detection System (IDS): deter, detect, document, deny, or delay intrusion by detecting a change in the environment.
- Security Forces: DoD, military, contract personnel, and trained dogs

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

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

If your CAC card is either lost or stolen, report it to your security office immediately (Kepler & Client)

Escort Requirements

- Ensure access to controlled areas by non-cleared personnel is minimal
- Only DoD civilians and contract and military personnel are authorized to escort non-cleared personnel
- Ensure all visitors sign the Visitor Log upon entry
- Check with your security office for specific escort procedures

Follow Client Site Guidance

Operations Security (OPSEC)

OPSEC: *Process to protect critical (classified or CUI) information from access by an adversary.*

OPSEC Practices:

- Remove ID badge when you leave your facility
- Do not post or send sensitive information over the web
- Guard against calls to obtain sensitive information
- Do not discuss sensitive information in public, or over the telephone
- Watch for and report suspicious activity

All Kepler Research employees must provide advance notice of foreign travel plans to the Security Office.

Foreign Travel Requirements

- **Notify your Kepler FSO and Gov't client's Security POC**
- Obtain defensive foreign travel security briefing prior to travel
- Obtain country specific briefing (if applicable)
- Current Antiterrorism/Force Protection Level 1 training (if required)
- Contact nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer if detained or subjected to harassment or provocation

SCI indoctrinated personnel must follow the previous steps.

Additional SCI Foreign Travel Requirements

- Complete foreign travel questionnaire
- Provide copy of itinerary
- Be aware of nearest U.S. Consulate, Defense Attaché, Embassy Regional Security Officer, or Post Duty Officer

Summary

- Personnel Security Clearance Process
- Information Security Program
- Pre-Publication Process
- Physical Security Program
- Operations Security (OPSEC) Program
- Understand the requirement for reporting foreign travel

KeplerResearch

Any Questions?