Industrial Security Briefing – Refresher 2016

Academy Solutions Group, LLC (ASG)

Glossary

CAPCO – Controlled Access Program Coordination Office

CDC – Cleared Defense Contractor

COR – Contracting Officer Representative

CSSO – Contractor Special Security Officer

DoD – Department of Defense

DSS – Defense Security Service

FSO – Facility Security Officer

IS – Information System

ITR – International Travel Request

NISPOM – National Industrial Security Program Operating Manual

PM – Program (or Project) Manager

SCI – Sensitive Compartmented Information

VR – Visit Request

Security Briefing Agenda

Per NISPOM, 3-106. Initial Security Briefings. *Prior to Being Granted Access to Classified Information, an Employee Shall Receive an Initial Security Briefing with periodic refresher briefings during each year that Includes the Following:*

A. A Threat Awareness Briefing/Insider Threat Briefing
B. A Defensive Security Briefing
C. An Overview of the Security Classification System
D. Employee Reporting Obligations and Requirements
E. Security Procedures and Duties Applicable to the Employee's Job

Additionally, we will cover the Special Security Agreement requirements.

Threat Awareness

Counterintelligence Threat

- United States defense-related technologies and information are under attack: each day, every hour, and from multiple sources.
- The attack is pervasive, relentless, and unfortunately, at times successful.
- As a result, the United States' technical lead, competitive edge, and strategic military advantage are at risk, and our national security interests could be compromised.
- Defeating this attack requires knowledge of the threat and diligence on the part of all personnel charged with protecting classified and controlled information, to deter or neutralize its effect.

Targeted Technologies

- DSS analysis of FY09 Suspicious Contact Reports indicated the following technologies, listed in descending order of foreign entity interest, represented probable collection priorities:
  - Information Systems
  - Aeronautics
  - Lasers and Optics
  - Sensors
  - Marine Systems
  - Positioning, Navigation, and Time
  - Electronics
  - Non-DSTL* Technology
  - Armaments and Energetic Materials
  - Materials and Processing

*** DoD's Developing Science & Technologies List**

Insider Threat

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.

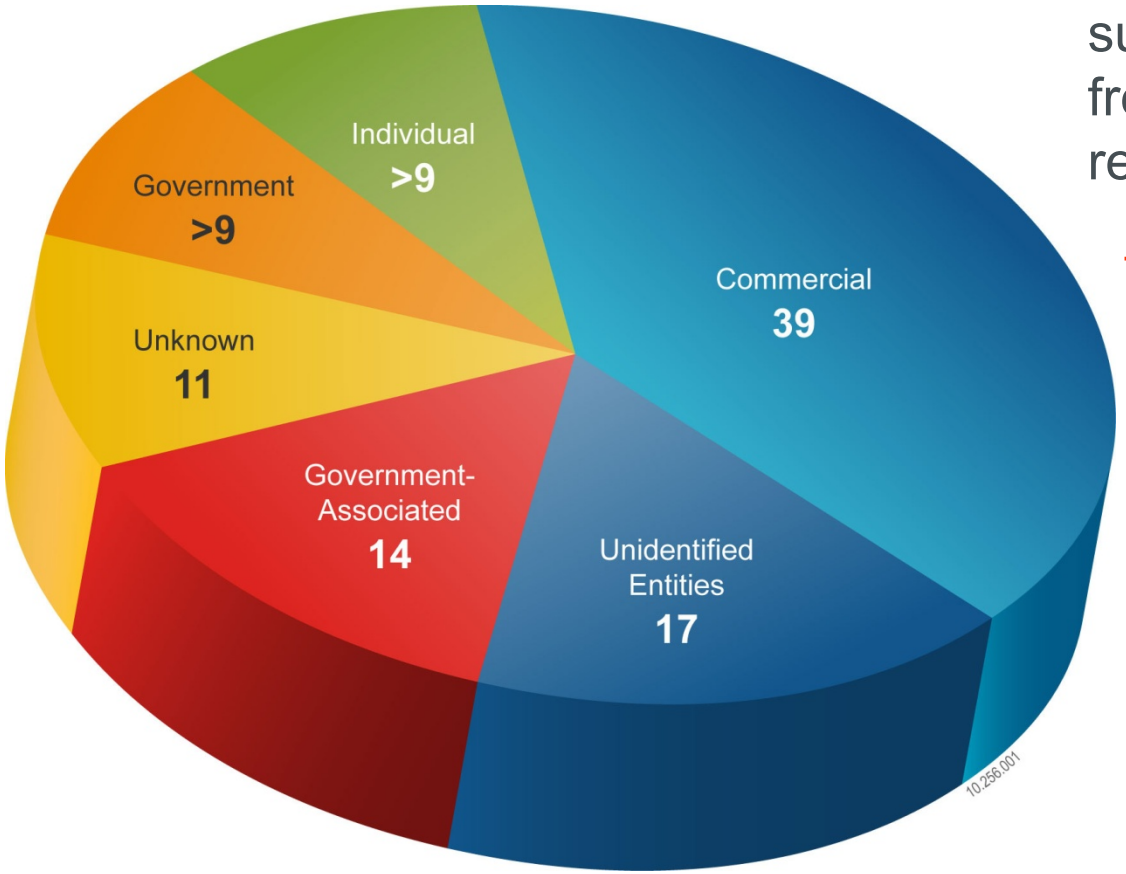
Potential Espionage Indicators:

- Failure to report overseas travel or contact with foreign nationals
- Engaging in classified conversation without a need to know
- Exploitable behavior traits
- Repeated security violations

Defensive Security Awareness

Counterintelligence Trends

Collector Affiliations - FY 2009
Percentages



- Targeting U.S. Technologies
- The collector affiliations suspicious entities most frequently used are represented in this figure
  - Commercial entities represented the top collectors of United States technology, outstripping government affiliated entities as the most frequently observed collector category

Top Four Collection Methods Used (FY09)

- Direct Requests
  - Email requests for information, web-card purchase requests, price quote requests, phone calls, or marketing surveys
- Suspicious Internet Activity
  - Confirmed intrusion, attempted intrusion, computer network attack, potential pre-attack, or spam
- Solicitation and Seeking Employment
  - Offering technical and business services to Cleared Defense Contractors (CDCs), resume submissions, or sales offers
- Foreign Visits and Targeting
  - Suspicious activity at a convention, unannounced visit to a CDC, solicitations to attend a convention, offers of paid travel to a seminar, targeting of travelers, questions beyond scope, or overt search and seizure

Foreign Travel Vulnerability

- Foreign Travel Increases the Risk of Foreign Intelligence Targeting
  - Collection Techniques Include:
    - Bugged hotel rooms or airline cabins
    - Intrusions or searches of hotel rooms, briefcases, luggage, etc.
    - Intercepts of fax and email transmissions
    - Recording of telephone calls/conversations
    - Unauthorized access and downloading, including outright theft of hardware and software
    - Installation of malicious software
    - Recruitment of substitution of flight attendants

Computer Security

- CDCs Provide Critical Research and Support to Programs Giving the U.S. an Economic, Technological, and Military Advantage in an Ever Increasing Global Economy
- Travelers Should Report Theft, Unauthorized or Attempted Access, Damage, and Evidence of Surreptitious Entry of their Portable Electronics
  - These effective counter-measures can decrease or prevent the loss of sensitive information:
    - Leave unnecessary electronic devices at home
    - Use designated ‘travel laptops’
    - Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
    - Ensure encryption is installed and running properly
    - Ensure no sensitive or controlled data exists on your desktop or hard drive

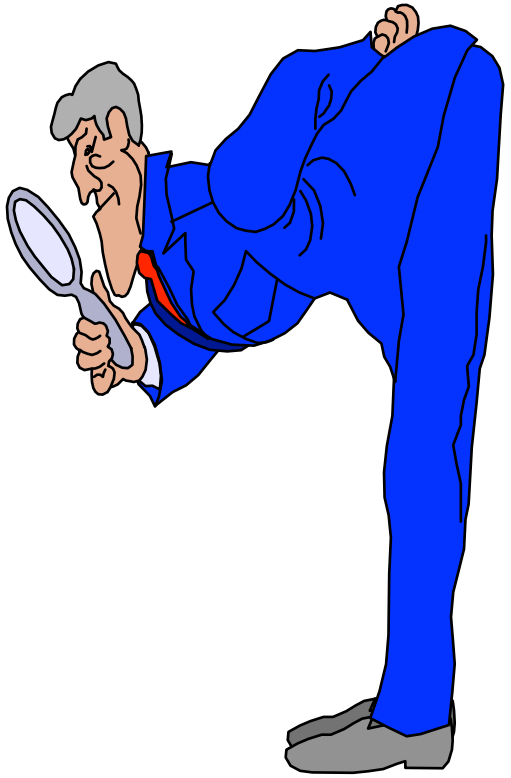
Security Classification Awareness

Protected Information

- **Top Secret -** Information or material, in which the unauthorized disclosure would cause "**EXCEPTIONALLY GRAVE**" damage to National Security.
- **Secret -** Information or material, that the unauthorized disclosure of which would cause "**SERIOUS**" damage to National Security.
- **Confidential -** Information or material, that the unauthorized disclosure of which would cause "**DAMAGE**" to National Security.
- **SCI –** Sensitive Compartmented Information
  - Protection of Sources and Methods
- **SAP –** Special Access Program
  - Any approved program that imposes need-to-know or access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET
- **COMSEC –** Communications Security
  - Secure communications utilizing NSA cryptographic material

Classified Information

- Must never be left unattended
- Must never be discussed in public places
- Must be discussed only on secure telephones or sent via secure faxes
- Must be under the constant control of an authorized person
- Must be stored in an approved location
- Must only be processed on an approved system
- Must not be removed or transferred without prior approval from the FSO/CSSO



Disclosure & Need to Know

- REMEMBER: Clearance + Need to Know = Access to Classified Information
- Need-to-Know is determined by the originator of the classified information
- Some customers may require Contracting Officer Representative (COR) approval before releasing classified
- If in doubt, contact your PM, FSO, or CSSO
- Gathering or Transmitting National Defense Information to, or on Behalf of, a Foreign Government is Punishable by Imprisonment or Death
- Failure to Report Such Occurrences, Allowing them to Occur through Gross Negligence, or Conspiracy to Defraud the U.S. is Punishable by Fines up to $10,000 or Prison Terms up to 10 years

Marking Classified

- Executive Order 13526, as amended, contains broad guidance on classification marking
- Controlled Access Program Coordination Office (CAPCO) maintains the register of approved Intelligence Community classification markings
- DoD 5200.1-R directs the application of approved markings to various types of documents/products
- DoD 5105.21-M-1 provides SCI marking guidance
- Required Markings
  - Overall Classification (most restrictive)
  - Portion Marking (e.g., titles, paragraphs, attachments)
  - Classification authority and declassification instructions (“Derived from:/Declassify on” block)
  - Mark each portion / paragraph / sub paragraph, etc., according to its content when standing alone
- Contact your FSO or CSSO with any questions

Disclosure of Contract-related Information

- Release of Information
  - Determined by DD254s for each contract
  - No Public Release is authorized without written approval IAW the DD254
- Public Disclosure
  - Neither confirm nor deny the validity of classified, sensitive, or customer information – even when it may appear in open-source publications, TV, media, or internet outlets
  - You must obtain advance approval from the customer and ASG Security prior to publishing or making public any information stated above (be sure to obtain your PM and VP approval prior to contacting the customer for public release authorization)
  - Open publication DOES NOT declassify the information
    - Inherently Government responsibility

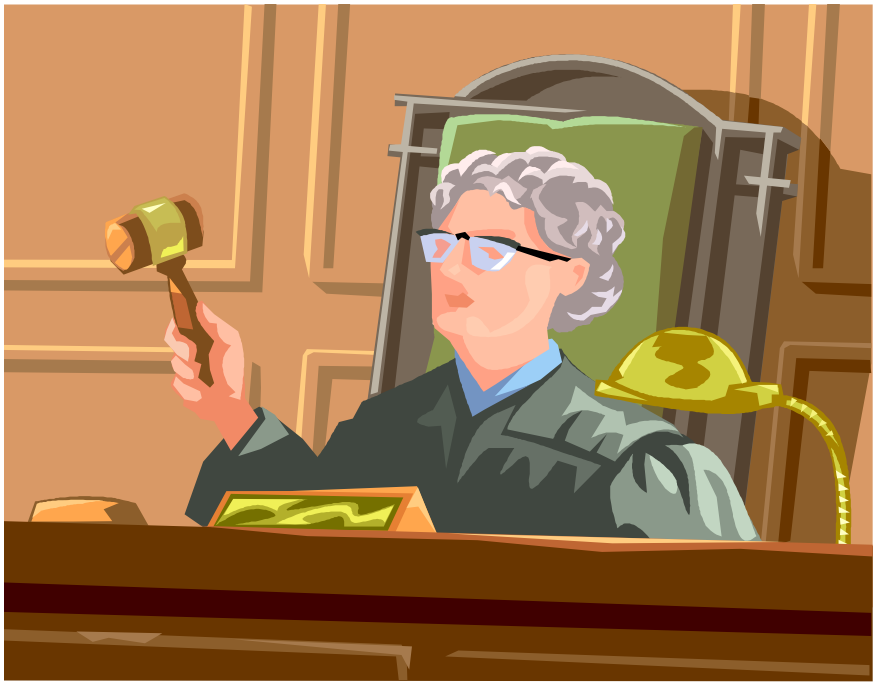
Transfer of Classified Materials

- TRANSFER METHODS APPROVED
  - Electronic
    - Classified e-mail must only be sent utilizing accredited systems
    - Classified faxes must be logged in accordance with local policies/procedures
  - Hand Carry
    - Requires advanced approval of your FSO or CSSO
    - Requires signed transmittal documents
    - Requires courier card and employee badge on your person at all times
  - Certified Defense Courier Service
    - Requires appropriate accounts and addressing
  - U.S. Mail
    - Confidential and Secret only (FedEx may be used with prior approval)

Always check with Customer Security prior to transferring or transporting classified materials to ensure all proper procedures, documentation, and wrapping/marking regulations are met.

Security Violations/Infractions

- Protecting our nation's classified data and information is critical
- Possible consequences of Minor violations:
  - Verbal Counseling
  - Written Counseling
  - Suspension/Termination
- Possible consequences of Major violations:
  - Same as minor violations
  - Loss of your security clearance
  - Arrest
  - Imprisonment or fines



Physical Security

- At least 5 days in advance of visiting other companies/facilities, ensure that you request that a Visit Request (VR) be sent
  - Depending on the contract you are on, the VR might be sent by your prime's CSSO, or possibly by your COR or government PM
- Badges
  - Should be worn at or above the waist, picture-side out
  - Only display the badge required/provided for the building you are visiting
- Ensure all local customer security policies and procedures are followed/met
  - Ensure you are aware of company or customer security practices and procedures and that they are followed consistently
  - Be aware you are subject to search when entering/leaving cleared facilities

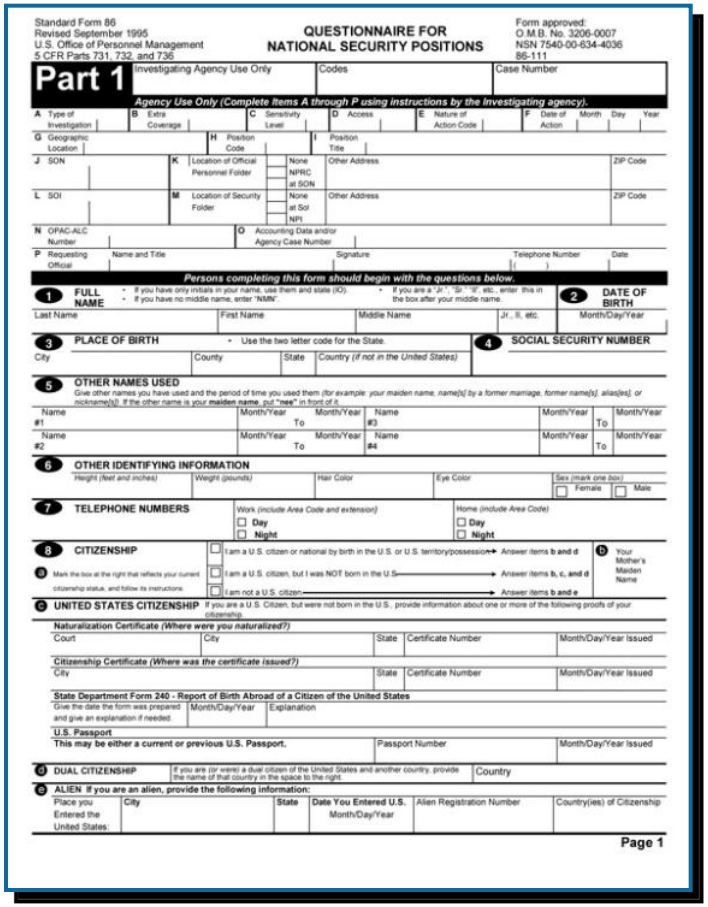
Computer Security

- Notify your FSO immediately if classified information is found on an unclassified system at your work location or ASG Security if classified information is found on any other unclassified system
  - DISCONNECT YOUR COMPUTER FROM THE LAN
  - DO NOT attempt to clean it yourself – wait for IS personnel to respond
  - DO NOT Delete, Forward, Print, or Save the information
- Phishing
  - Do you see anything wrong with the addresses below?
    - Bill-smith@Lockheedsmartin.com
    - CustomerSupport@ebay-bilLing.com
    - Notice@bankofamer1ca.com
- Be aware of your actions and communications
- Do not open attachments or follow hyperlinks unless you are expecting them from a confirmed/trusted sender

Employee Reporting Obligations

Reporting Requirements

- **ANY CHANGE** in status (since last investigation) **MUST** be reported:
  - Security violations/infractions
  - Change in marital status
  - Adult cohabitation
  - Psychological counseling (other than marital, career, or grief)
  - Financial problems, garnishments, bankruptcy, late payments (excessive indebtedness), or sudden affluence
  - Close or continuing foreign contacts
  - Litigations, charges, arrests, court summons – ANY involvement with police
  - Application or possession of a foreign passport



Standard Form 86
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
O.M.B. No. 3206-0007
NSN 7540-00-634-4036
86-111

Part 1

Investigating Agency Use Only | Codes | Case Number

Agency Use Only (Complete Items A through P using instructions by the investigating agency).

A Type of Investigation | B Extra Coverage | C Sensitivity Level | D Access | E Nature of Action Code | F Date of Action (Month Day Year)

G Geographic Location | H Position Code | I Position Title

J SON | K Location of Official Personnel Folder (None / NPRC at SON) | Other Address | ZIP Code

L SOI | M Location of Security Folder (None / at SOI / NPI) | Other Address | ZIP Code

N OPAC-ALC Number | O Accounting Data and/or Agency Case Number

P Requesting Official | Name and Title | Signature | Telephone Number | Date

Persons completing this form should begin with the questions below.

1 FULL NAME — If you have only initials in your name, use them and state (IO). If you have no middle name, enter "NMN". If you are a "Jr.", "Sr.", "II", etc., enter this in the box after your middle name.
Last Name | First Name | Middle Name | Jr., II, etc.

2 DATE OF BIRTH
Month/Day/Year

3 PLACE OF BIRTH — Use the two letter code for the State.
City | County | State | Country (if not in the United States)

4 SOCIAL SECURITY NUMBER

5 OTHER NAMES USED
Give other names you have used and the period of time you used them (for example: your maiden name, name(s) by a former marriage, former name(s), alias(es), or nickname(s)). If the other name is your maiden name, put "nee" in front of it.
Name #1 | Month/Year To Month/Year
Name #2 | Month/Year To Month/Year
Name #3 | Month/Year To Month/Year
Name #4 | Month/Year To Month/Year

6 OTHER IDENTIFYING INFORMATION
Height (feet and inches) | Weight (pounds) | Hair Color | Eye Color | Sex (mark one box): Female / Male

7 TELEPHONE NUMBERS
Work (include Area Code and extension): Day / Night
Home (include Area Code): Day / Night

8 CITIZENSHIP
Mark the box at the right that reflects your current citizenship status, and follow its instructions.
I am a U.S. citizen or national by birth in the U.S. or U.S. territory/possession → Answer items b and d
I am a U.S. citizen, but I was NOT born in the U.S. → Answer items b, c, and d
I am not a U.S. citizen → Answer items b and e
b Your Mother's Maiden Name

c UNITED STATES CITIZENSHIP — If you are a U.S. Citizen, but were not born in the U.S., provide information about one or more of the following proofs of your citizenship.
Naturalization Certificate (Where were you naturalized?): Court | City | State | Certificate Number | Month/Day/Year Issued
Citizenship Certificate (Where was the certificate issued?): City | State | Certificate Number | Month/Day/Year Issued
State Department Form 240 - Report of Birth Abroad of a Citizen of the United States: Give the date the form was prepared and give an explanation if needed. | Month/Day/Year | Explanation
U.S. Passport: This may be either a current or previous U.S. Passport. | Passport Number | Month/Day/Year Issued

d DUAL CITIZENSHIP — If you are (or were) a dual citizen of the United States and another country, provide the name of that country in the space to the right. | Country

e ALIEN If you are an alien, provide the following information:
Place you Entered the United States: | City | State | Date You Entered U.S. Month/Day/Year | Alien Registration Number | Country(ies) of Citizenship

Page 1

Adverse Information

- **Any information that reflects on the integrity or character of a cleared employee that indicates their capability of safeguarding classified material. Samples are below; if you have doubt contact Security.**
- **Any convictions of wrongdoings**
  - other than a simple traffic stop/ticket
- **Any arrests resulting in a summons**
  - Driving while intoxicated
  - Driving under the influence
  - All illegal drug charges
  - Domestic Violence
- **Any financial difficulties**
  - Bad Check Conviction
  - Late payment of 60-90 days or greater
  - Bankruptcy
- **Hospitalization for Mental or Emotional Problems**
- **Membership in Subversive Organizations**
- **Security Violations or Compromises**

Suspicious Contact Reporting

- Suspicious contacts include:
  - Unsolicited requests for detailed information about
    - Your Job
    - Security Clearance
    - Contract, Sensitive, or Proprietary Information
    - Technology
- Information requests that seem out of place, unusual, very pointed/ specific, or out of the ordinary should be reported immediately
  - Report to ASG Security immediately
    - Potential to be routed to Government
    - Do not discuss classified or controlled information with family members or anyone else without a confirmed need-to-know established

National Reporting

- Where to report Fraud, Waste, Abuse, Unauthorized Disclosures (leaks), Human Trafficking, and Threats to Homeland & National Security
  - DoD: 800-424-9098 or e-mail to hotline@dodig.osd.mil or their website at http://www.dodig.osd.mil/hotline
    - Posted in break rooms and common areas throughout cleared facilities
- You should also contact your FSO or CSSO
- Report to your FSO or CSSO the receipt of classified material from foreign interests not received through government channels
- Report immediately to your FSO or CSSO any information coming to your attention concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations – Security has an obligation to forward a written report to the FBI

Security Procedures and Duties

Secured Areas

- Inadvertent Disclosure
  - Involuntary unauthorized access to classified information to an individual without a clearance/access
    - Notify your FSO/CSSO immediately
  - Personal Responsibilities
    - Notify Security immediately
      - Contain/control the situation/material immediately
      - Assist in the investigation as directed by your FSO/CSSO
- During Emergencies
  - Always grant unimpeded access to emergency personnel (police, fire, medical)
    - Ensure and confirm your FSO/CSSO has been notified so they may get a count of emergency personnel entering the facility

Nondisclosure Agreement (SF 312)

- All persons authorized access to classified information are required to sign a nondisclosure agreement as a condition of that access. The SF 312 is a contractual agreement between the U.S. Government and you.
- ASG personnel are bound by DoD rules and regulations to properly protect and control all classified material in our possession.
- Your Three Lifetime Obligations:
  - SAFEGUARD PROTECTED INFORMATION
  - PREPUBLICATION REVIEW
  - REPORTING UNAUTHORIZED DISCLOSURE OF PROTECTED INFORMATION

Laptop Computers & Foreign Travel

- Contact ASG Security prior to taking your laptop with you on foreign travel
  - Travel briefings are required
    - Laptops are high theft items – protect it!
      Report theft or unauthorized access to ASG Security immediately
  - Software encryption must be activated
- ASG must ensure compliance with U.S. export laws for:
  - International Trade
  - Technology Transfer

Foreign Travel

- Foreign Travel Tips
  - Do not make reference to your intelligence affiliation or access to classified information
  - Do not take your laptop unless you have proper approvals
  - Maintain a low profile
  - Do not photograph military or defense areas or equipment
  - Refer to the State Department website for specifics on travel warnings, updates, health, and other issues
- An International Travel Request (ITR) form and a Defensive Travel Briefing is required for all business-related foreign travel and travel by all cleared personnel - it is strongly recommended for personal travel as well

National Security

ASG Security

CSSO:

Greg Whaley

office: 410-290-0871, ext. 204

cell: 443-812-9639

fax: 410-290-0874

Alternate CSSO:

Steve Hubbard

office: 301-543-5161

cell: 301-346-9106

Refresher Briefing Acknowledgement 2016

I hereby certify that I have received the Refresher Security Briefing and I understand the importance of safe-guarding classified information, reporting adverse actions to my FSO/ CSSO, and agree to comply with all NISPOM security regulations. I understand that protecting classified and/or contractual information is paramount to both the success of my contract and the continued support of this country. I further understand that this briefing does not address every security responsibility or issue that I must be aware of, but instead is a broad overview of my security responsibilities. Additionally, I understand that I am required to participate in a continuing security training program as provided by ASG Security, and to update my contact information if it changes from what I've provided below.

_____ _____

Employee Signature Today's Date

_____

Employee Printed Name

Please print this page, sign & date it, and submit it (via hard copy or fax) to the alt. CSSO or the CSSO by COB 31 January 2017.