Annual Industrial Security and Export Compliance Briefing 2017

This briefing is unclassified

Presented by:

Jamie Fisher, FSO

Contact information

FSO contact:
Jamie Fisher jfisher@innssi.com
937-630-3012 x100

Export Controlled contacts:
Steve Palluconi spalluconi@innssi.com
937-630-3012 x104
Grant McMillan gmcmillan@innssi.com
937-630-3012 x106

DSS Rep
Richard Legere
Special Agent
Industrial Security Representative
Defense Security Service
937-320-8315(Office)

DSS Hotline
800-424-9098
hotline@dodig.osd.mil
http://www.dodig.mil/hotline

Welcome to your annual security refresher training. The purpose of this briefing is to remind you of your personal responsibilities and liabilities under United States espionage and sabotage acts, and to reaffirm key security policies and procedures. The protection and safeguarding of classified information is all of our responsibilities.

Refresher topics

Welcome to your annual training! The topics you will review are….

- -Your Obligation
- -Classified and Unclassified Information
- -Collection Trends
- -Safeguarding Classified Information
- -Visitors
- -Travel
- -Internet Security
- -Global Economy
- -Reporting Requirements
- -Infractions and Violations
- -Insider Threat Awareness
- -Export Compliance

Your Obligation

- When you received your security clearance, you signed a non-disclosure agreement form. By signing this form you agreed to:

  -Accept a lifelong obligation to protect classified and sensitive government information.
  -to submit any writing for pre-publication review

- You vowed to avoid unauthorized disclosure, retention, or negligent handling of sensitive materials
- You also verified, by your signature; that you understood the consequences of violating the non-disclosure agreement

Legal and Binding

There are two titles on the NDA that provide specific punishments for violation, statues of Title 18 and Title 50 can lead to:

- Prison sentences
- Fines
- Or both

Annual refresher training is provided to you as a protection measure and reminder of appropriate handling measures, your reporting requirements, and responsibilities as a cleared employee, and as a result of signed the NDA.

For more information on these titles, visit the website shown:
-For title 18: http://uscode.house.gov/browse/prelim@title18&edition=prelim
-For title 50: http://uscode.house/gov/browse/prelim@title50/chapter23&edition=prelim

Type of Government Information

There are two categories of government information that you may deal with at your current job responsibilities.

-Unclassified-is material that does not require a security clearance and,

-Classified-material that does require special clearances and considerations to have access

Unclassified Government Information

Unclassified material can be very sensitive information to our company and your job duties. In some cases, the material may have special handling and destruction requirements. Unclassified material that is co-mingled with classified material must be marked unclassified.

This type of data will normally be marked For Official Use Only (FOUO). Another unclassified marking is Control Unclassified Information (CUI). These types of information are not for public disclosure.

The statement of work provided with tasking or the overall contract document will provide specific instructions on the handling of these types of materials. For further guidance, check with your program manager, supervisor, or contracting officer, if you have materials that contain these types of marking labels.

Classified Government Information

There are three distinct levels of classification within the Department of Defense system.
-**Confidential**-is information, that when compromised could expect to cause damage to our national security
-**Secret**-is information, that when compromised, could result in grave damage to our national security
-**Top Secret**-is information, that when compromised, could result in exceptionally grave damage to our national security
To access any of these three types of information, you must have a clearance at that level or higher and a valid need to know. Employees are responsible for familiarizing themselves with the classification guides and directives associated with the program they are supporting. When creating a classified document it is the originator's responsibility to determine the appropriate classification level. When you are unsure how to interpret the classification guide, discuss with your supervisor or manager.

Classified Government Information

When creating classified material be aware that there are two types:

-Originally classified, is that material classified by a government official, designated in writing by the president of the United States. Or,

-Derivatively classified material. As a cleared contractor material created is derived by a source document or documents, or from guidance provided by a security classification guide or government directive form known as DD 254.

If an employee believes that information is classified improperly or unnecessarily, the classification may be challenged, or a determination made through program security and the government contracting agency or original classifying agency. In addition, as a holder of these materials, you are required to limit access to the information to those that have a need to know. By enforcing this, need to know principle, you will limit the chances that the classified information, could be compromised through inadvertent disclosure or release, and in turn keeps our nation and its secrets more secure.

Collection Trends

The first known collection efforts occurred several hundred years ago, and continue today. In recent years collection efforts have become more focused on dual use technologies. Reports indicate that the extent of foreign interest in specific categories of technology varies dramatically from country to country, and the leading edge technologies are not the only technologies being targeted.

Countries with less developed industrial sectors often prefer older, off the shelf hardware and software that costs much less and is more suitable, for integration into their military programs. This lends additional credibility to using care when providing information to foreign nationals, since you may not always be aware of its end use.

Economic Espionage

The American society of Industrial Security recently conducted a survey of trade secret theft. This survey found, that the most common targets were customer related information, such as:

- -Business volume and preferences
- -Financial data
- -New product information
- -Manufacturing process information

Use caution when sharing these types of information during times you may be working with our competitors.

Protecting Classified Materials

Our diligence in exercising the need-to-know principle, by restricting access to the material you possess, plays a key role in the prevention of potential espionage. Most spies reported that they were able to obtain more information than they were initially seeking.

Always maintain direct control of classified and sensitive information and mark materials properly.

- Must be under constant personal custody
- Must never be discussed in public places
- Must be discussed on secure phones
- Must never be left unattended
- Must be stored in GSA approved storage containers
- Must never be process on your computer unless approved

Handling Visitors

Identify:

- -clearance level of visitor
- -Status of the visitor
  - -Citizenship
  - -Program involvement
- -Restrictions required by that specific area

As a sponsor for a visitor, you should ensure that your visitor understands any restrictions or requirements placed upon their visit to the facility. All foreign visitors must be coordinated and approved by Export Compliance prior to the visit. For specific requirements about signing in a visitor to your site or classified area check with the security officer primarily responsible for that area.

Travel

RQ's overseas travel webpage is https://rqintranet.wpafb.af.mil/rqoogle/content.cfm?cid=193.

OSI's webpage is https://cs.eis.af.mil/sites/10455/ci/ftb/10%20FIS/_layouts/15/viewlsts.aspx?BaseType=4.

Please complete the Pre-Travel and Post-Travel questionnaires.

If attending a conference within the states please complete the Domestic Conference Travel questionnaire from the OSI webpage. The Domestic Conference Travel questionnaire is AFOSI's newest initiative to protect personnel from foreign threats while traveling domestically for official business. It has been added to their SharePoint site to help them identify where people are traveling to better prepare them for what they might encounter.

Travel

AFI10-245 requires all government civilians and military members receive the appropriate threat awareness information prior to departure. You are also required to complete AT level I awareness training, if not completed within the last year. Note, this is the annual training you take titled Force Protection (ZZ133079). It can be found in ADLS. Please visit this website https://cs.eis.afmc.af.mil/sites/AT-FP/wpafb/Travel/default.aspx and follow the instructions provided. Should you have any questions or concerns please feel free to contact Deirek King.

If you have been briefed into SCI control channels you will need to contact Deirek King as you are required to submit additional documentation.

Another good source is https://www.fcg.pentagon.mil as well as the state department's webpage at http://travel.state.gov.

Once you complete the pre-travel questionnaire let me know and I will send over ISSI's pre-travel briefing for signature.

Internet Security

When utilizing your company computer on the internet, don't draw attention to yourself, or your clearance by surfing foreign intelligence sites, or sites that are fishing for individuals with specific clearance level.

Be careful what you download. If you must download a file or application, make sure it's from a trusted and secure site. Avoid accessing sites that post speculative information.

And, above all, remember, there is no security on the internet.

Working in a Global Economy

As an employee of a Government Contractor, you should not avoid contact with foreign nationals, or distrust all persons from abroad. Your encounters with foreign colleagues and cultures should be among your most treasured experiences. However, you must always be aware, that among millions of foreigners who come to our country, or whose countries you visit, there are some who would exploit your trust.

Reporting Requirements

- Change of personal status: marital status, name change, cohabitation of an intimate nature
- Adverse information—arrests, criminal activities, use of drugs, out of character behavior, or treatment for emotional or mental disorders, recurring financial difficulties or excessive debtedness
- Known or suspected espionage or sabotage—suspicious contacts
- Becoming a representative of a foreign interest
- Known or suspected compromise of classified information
- Close and continuing relationships with foreign nationals

Infractions and Violations

Unfortunately, when dealing with classified information there can be security incidents, infractions, or violations. Types of these that occur most frequently are:

-classified are left unsecured
-allowing an uncleared individual into an area
-introduction of prohibited items
-classified material removed without proper authorization; and
-data spillage
    -pay attention when using classified computer systems
    -know what is classified. Become familiar with the classification guide

Employees must report any non-compliance or willful/gross neglect of security requirements or procedures. Employees are encouraged and expected to report any information that raises doubts about another employee's continued eligibility for access to classified information. Report any information regarding actual or potential acts of espionage, sabotage, or terrorism.

Insider Threat Awareness

Please review the Insider Threat Awareness training at the link below:

https://securityawareness.usalearning.gov/itawareness/build/index.html

Export Compliance – A Critical Requirement for ISSI

- Foreign sales is the fastest growing component of ISSI's commercial product success.
- Although profitable, exporting involves potential threats to national security.
- Compliance with U.S. export regulations is carefully monitored by multiple organizations within the Dept. of State, Dept. of Commerce, Dept. of Treasury and the Census Bureau.
- ISSI has in place an Export Compliance Management System consistent with federal requirements.
- **One requirement is that all ISSI employees have recurring training and develop basic familiarity with this program.**

What ISSI Base Employees Need to Know

- The U.S. Government takes export laws very seriously.
- Penalties for non-compliance are steep and can be ruinous to a small business.
- Penalties can be levied on ISSI and/or on individual employees who were responsible for the violation.
- Non-compliance by ISSI's Commercial Products Group could directly impact our ability to engage in government contracting.
- Non-compliance by ISSI Base employees could result in ISSI's debarment from exporting.
- **Base employees can violate U.S. export laws even though you have no relationship to ISSI foreign sales.**

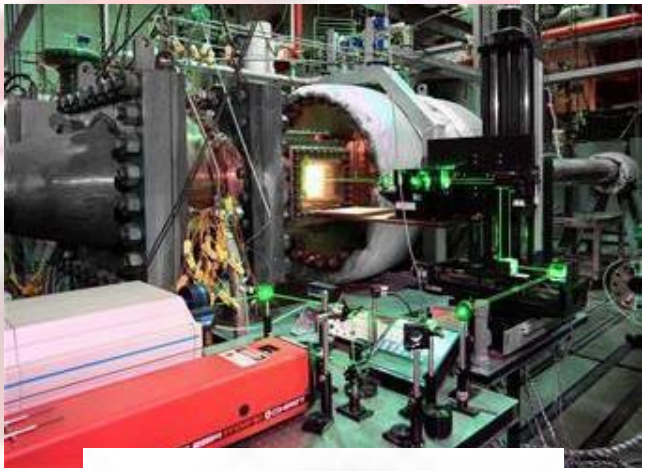
A Broad Range of Items are Subject to Export Controls…

Exports can be …

- **Physical** – taking / sending / giving a part / data to a foreign country or person.
- **Verbal** - telling foreign person information about a controlled part / data.
- **Visual** - a foreign person seeing controlled information – even if they see it on your laptop in a public place.

Potential Export Violations

- Providing technical data (drawings, specifications) on USAF test facilities to a component supplier or subcontractor without identifying its export controls.
  - Without export control markings the component supplier/subcontractor could inadvertently provide them to a foreign source.
  - Always work with Tracy Frecker and inform her of the source of the drawings or specifications.
- Failure to use encryption when providing controlled data electronically, even though it includes the export control markings.
- Bringing a laptop or tablet on overseas travel with export controlled data on it.

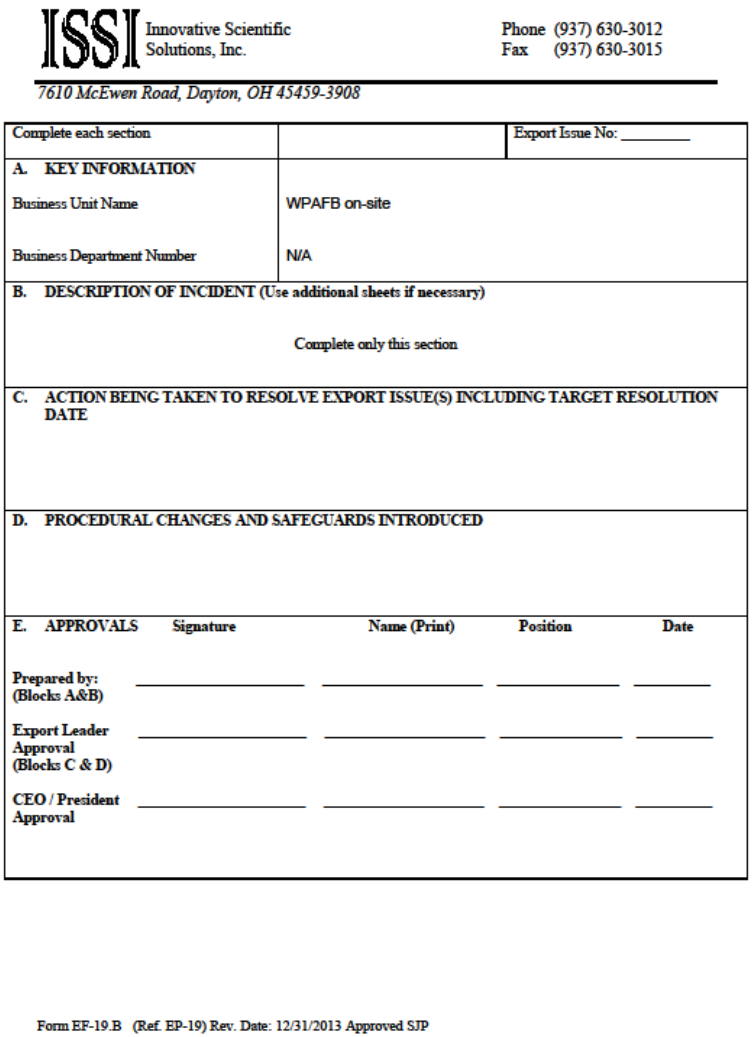


Organizational Responsibilities

- ***Employees are strictly prohibited from acting on their own***, to provide, disclose, or share export controlled information, grant access, describe export control policies and procedures.
- ***Employees are strictly prohibited from*** interpreting export control regulations.
- ***Employees are strictly prohibited from*** **responding to any request from customers or regulatory government authorities** regarding export controls.
- Empowered Official (Steve Palluconi) and Export Compliance Officer (Grant McMillan) are the only employees authorized to respond to inquiries and requests from government regulatory authorities.

Reporting Suspected Violations (Hotline Numbers)

- If comfortable doing so, employees can report suspected violations directly to Steve Palluconi (Empowered Official) or Grant McMillan (Export Compliance Officer).
- If an employee prefers to make an anonymous report, they can use Form EF-19.B. A copy is available on the Employee Portal of the ISSI website (www.innssi.com) Only fill out the description of the incident (Section B).



ISSI Innovative Scientific Solutions, Inc.

Phone (937) 630-3012
Fax (937) 630-3015

7610 McEwen Road, Dayton, OH 45459-3908

Complete each section		Export Issue No: _____
A. KEY INFORMATION		
Business Unit Name	WPAFB on-site	
Business Department Number	N/A	
B. DESCRIPTION OF INCIDENT (Use additional sheets if necessary)		
Complete only this section		
C. ACTION BEING TAKEN TO RESOLVE EXPORT ISSUE(S) INCLUDING TARGET RESOLUTION DATE		
D. PROCEDURAL CHANGES AND SAFEGUARDS INTRODUCED		

E. APPROVALS	**Signature**	**Name (Print)**	**Position**	**Date**
Prepared by: (Blocks A&B)				
Export Leader Approval (Blocks C & D)				
CEO / President Approval				

Form EF-19.B (Ref. EP-19) Rev. Date: 12/31/2013 Approved SJP

Reporting Suspected Violations (Hotline Numbers)

- Defense Department 1-800-424-9098
- Defense Intelligence Agency 703-907-1307
- National Security Agency 301-688-6911
- Department of Army 1-800-225-5779
- Naval Criminal Investigative Service 1-800-543-6289
- Air Force Office of Special Investigations 202-767-5199
- Central Intelligence Agency Office of the Inspector General 703-874-2600
- Department of Energy 202-586-1247
- US Nuclear Regulatory Commission Office of the Inspector General 1-800-233-3497
- US Customs Service 1-800-232-5378
- Department of Commerce/Office of Export Enforcement 202-482-1208
- Department of State Bureau of Diplomatic Security 202-663-0739
- When traveling overseas, suspect incidents should be reported to the Regional Security Officer (RSO) or Post Security Officer (PSO) at the nearest U.S. Diplomatic Facility

Certification

I have received, reviewed and understand the contents of this industrial security and export compliance briefing. Any questions that I raised were addressed by ISSI's FSO and EO.

Print Name: _____

Signature:_____

Date:_____