Annual Industrial Security and Export Compliance Briefing 2016

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….

-Clear Facility
-Personnel Security Clearance Eligibility Criteria
-Cleared Personnel
-What is Classified Information?
-Levels of Classified Information
-Safeguarding of Classified Information
-Security Violations
-Counterintelligence Awareness
-Individual Reporting Requirements
-Foreign Travel
-Infractions and Violations
-Export Compliance

Cleared Facility

- A Facility Clearance (FCL) is a determination that a company is eligible for access to classified information or award of classified contract. This process involves an evaluation of the corporation organization; key leadership; outside corporate relationships; foreign influence; etc.
- Companies are required to complete a DOD SECURITY AGREEMENT (DD Form 441) which outlines its security responsibilities.
- As a defense contractor, we are bound by Department of Defense (DOD) rules and regulations to properly protect and control all classified material in our possession. We are authorized to accept and safeguard classified information and materials.
- You, as an employee, are equally bound under the law to provide the same protection and control.

Personnel Security Clearance Eligibility Criteria

Security judgement is based on pattern behavior, not a single action. It's the "whole person" concept. The 13 Adjudication Guidelines and examples of activities reviewed are:

- Allegiance to US—Sabotage, espionage, treason, terrorism. Statements actions that show allegiance to other than US
- Foreign Influence—Unreported personal contacts with foreign intel service, government or persons seeking classified information.
- Foreign Preference—Foreign national family members or close contacts. Exercise of any right, privilege or obligation of foreign citizenship.
- Sexual Behavior—Criminal sexual behavior. Compulsive, self-destructive and high risk behavior that you are unable to stop
- Personal Conduct—Recurring pattern of poor judgement, irresponsible or unstable behavior. Deliberate omission of falsification of information on a security questionnaire.
- Financial Consideration—Not pay bills. Living beyond your means. Not filing tax returns (tax evasion). Bankruptcy.

Personnel Security Clearance Eligibility Criteria

- Alcohol Consumption—DUI/DWI. Irresponsible behavior while intoxicated. Concealment of drugs or alcohol while at work.
- Drug Involvement—Use of illegal/illicit drugs. Positive drug test for illegal/illicit drugs. Misuse of prescription drugs.
  - NOTE: Possessing and using Marijuana is legal in some states but it is still a federal crime and will impact your clearance.
- Psychological Conditions—Problematic behavior not addressed through counseling or other professional services.
- Criminal Conduct—Arrest. Spousal or child abuse/neglect. Pattern of disregard for rules and regulations.
- Handling Protected Information—Unauthorized disclosure. Taking/sending classified information home. Downloading info to an unapproved system.
- Outside Activities—Service/employment, paid or unpaid, with a foreign government or representative/person of a foreign interest.
- Use of Information Technology Systems—Unauthorized entry into any compartmented system. Attempting to circumvent or defeat security of auditing systems. Introduction, removal, or duplication of hardware/software or media to or from system without authorization.

Cleared Personnel

- Department of Defense Central Adjudication Facility (DoD CAF) grants a security clearance based upon the personal information provided on your application (eQIP) and appropriate back ground investigation.
- Access to information is restricted based upon the person's status: Citizen of the United States; Lawful Permanent Resident Alien; or a foreign national authorized to work in the U.S.

Position	Legal Status	Access Levels Allowed
Requires access to classified information	US Citizen	Secret, Top Secret, SCI
Requires access to Controlled Unclassified Information (CUI)	US Citizen Lawful Permanent Resident Aliens	CUI—no government IT systems or technical data access
Requires access to CUI/Government IT Systems/ITAR Technical Data	US Citizen	CUI/Government IT Systems/ITAR Technical Data
General Positions—no access to classified information	Anyone authorized to work in the U.S.	Low sensitivity informaton

Cleared Personnel

- Once cleared, you are required to sign a non-disclosure contract (SF312) with the US Government.

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 13526, 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 13526, 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.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

STANDARD FORM 312 (Rev. 7-2013)
Prescribed by ODNI
32 CFR PART 2001.80 E.O. 13526

Cleared Personnel

- The SF312 is a contractual agreement between the U.S. Government and you. The primary purpose of the SF312 is to inform you that:
  - A special trust has been placed in you;
  - This agreement is binding upon you and for life (even if you no longer require a security clearance);
  - You are responsible to protect classified information from unauthorized disclosure; and
  - There are serious consequences for not complying with the terms of this agreement.

Cleared Personnel

- All cleared employees will receive some form of security briefing—whether Indoctrination; Orientation; Refresher or other prior to accessing classified information
- Dependent upon your specific job and location, security procedures will be based upon instructions provided by the client through DD 254; Classification Guide or other instruction/requirement stated in contracts.
- All employees must comply with the client security requirements to include security briefings; access to client provided IT systems and classified information.
- A violation of client security policies and procedures may be grounds for removal from the contract.

What is Classified Information?

- Classified Information is that information, the unauthorized disclosure of which could adversely affect the national security of the United States. The information is usually owned by, produced by, or for or under the control of the U.S. Government, and meets the criteria of Executive Order 12356.

Levels of Classified Information

- Top Secret—The unauthorized disclosure of information will cause exceptionally grave damage to the U.S. National Security.
- Secret—The unauthorized disclosure of information will cause serious damage to U.S. National Security.
- Confidential—The unauthorized disclosure will cause damage to U.S. National Security
- There are other categories of information which, while not classified, also deserve mention:
  - For Official Use Only (FOUO)—is unclassified government information which is exempt from general public disclosure and must not be given general circulation
  - Company private or proprietary information—is business information not to be divulged to individuals outside the company.
  - Recently DoD has placed great emphasis on protecting Controlled Unclassified Technical Information. The treatment of this type of information will be addressed on the following slides.

Levels of Classified Information

Controlled unclassified technical information—means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. There are no exceptions for commercial items.

- Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Contractors are required to safeguard unclassified controlled technical information and to report the compromise of such information to the DoD within 72 hours of discovery.

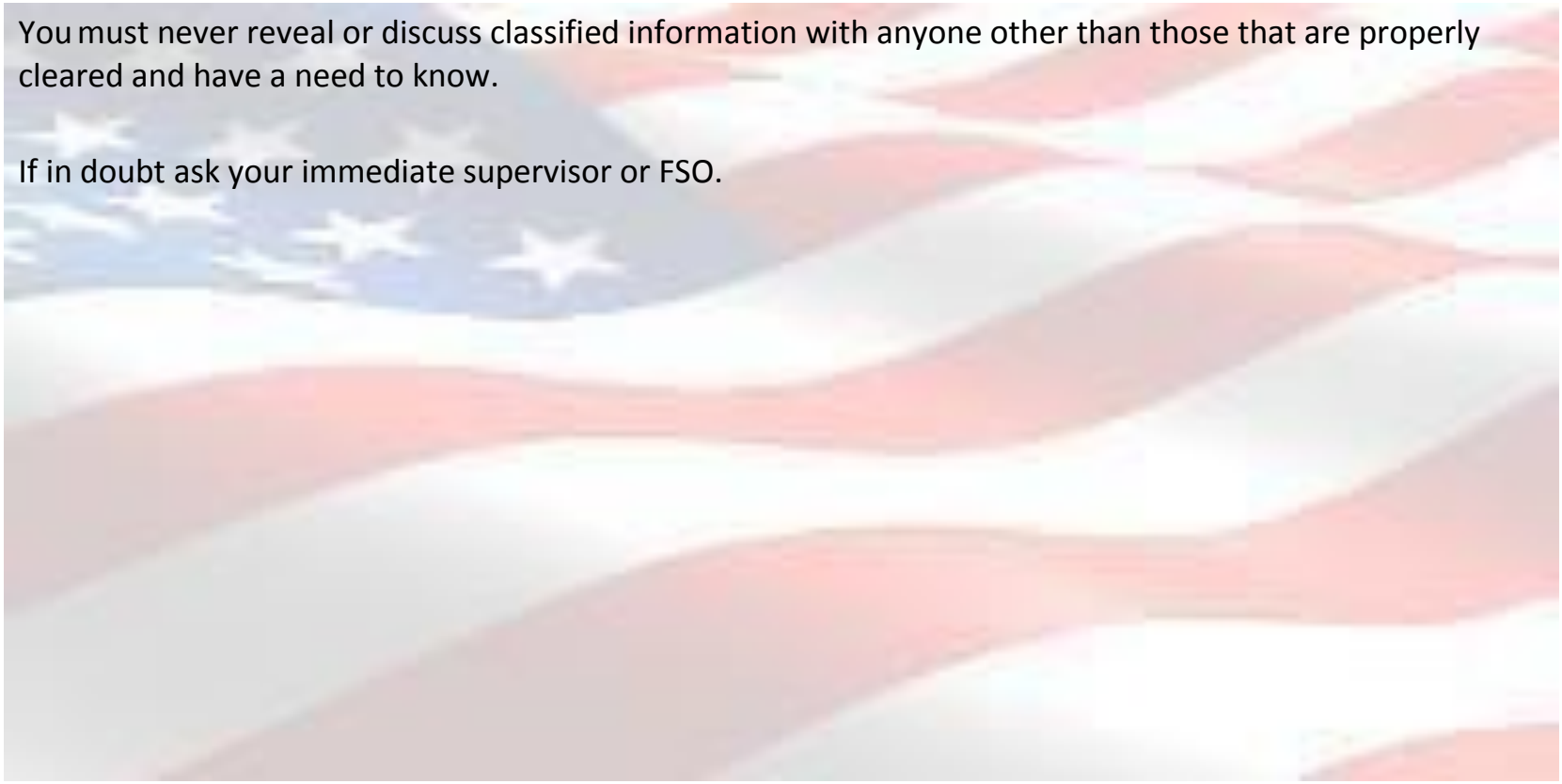
Contractors subject to the clause are required to implement data security controls identified in National Institute of Standards and Security (NIST) publication SP 800-53.

Contractors are responsible for assuring that their subcontractors that are provided with controlled technical information also comply with the data security standards. The new contract clause is a mandatory “flow-down” clause to subcontractors. This includes so-called “cloud” storage providers.

Safeguarding of Classified Information

- 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

Safeguarding of Classified Information



You must never reveal or discuss classified information with anyone other than those that are properly cleared and have a need to know.

If in doubt ask your immediate supervisor or FSO.

Security Violations

- Minor Violations MAY include:
  - Verbal Counseling
  - Written Counseling
- Major Violations MAY include:
  - Same as minor violations
  - Loss of employment
  - Loss of your security clearance
  - Arrest
  - Imprisonment or fines

Be Aware

There are representatives from other nations whose goal is to obtain classified information and to utilize that information to their own advantage, and to damage US National Security. A clear line must be drawn to protect classified information; anything that is subject to export controls; proprietary information; and controlled unclassified technology.

- Two most common approaches are:
  - Coercion/Blackmail
  - Cultivation of Relationship

Counterintelligence Awareness

Other approaches include:

- Suspicious Network Activity
  - Cyber Intrusion; Viruses/Malware; Backdoor Attacks; Acquiring User Names/Passwords
- Attempted Acquisition of Technology
  - Front Companies for 3rd Parties; Protected Info; Controlled Technologies; Equipment; Diagrams; Plans
- Request for Information
  - Attempt to get info through price quotes or market surveys
- Solicitation or Marketing Services
  - Foreign entities through sales, rep or agency offers; RFI/RFP responses for technical or business services
- Seeking Employment
  - Resume submissions, applications and references

If you encounter any of these situations that seem suspicious, contact your security officer.

What are we defending?

Information concerning military capabilities, locations, equipment; and technology is protected for a reason. Unauthorized release of this information, whether classified or sensitive can have a detrimental effect on the Warfighter's survivability.

Individual 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

Foreign Travel

- You must report all Foreign Travel and a Foreign Travel briefing is required. Personnel holding TS/SCI may have additional reporting requirements. Check with your government client or FSO. It is your responsibility to make those arrangements BEFORE you leave.
- You will need to complete the briefing, by signing and returning to the FSO prior to leaving. This can be discussed via telephone as well. Once you return, you will be debriefed.
- Develop a personal travel plan and give it your immediate supervisor and family
- Learn the cultures, customs and laws of the country you visit
- Visit http://www.state.gov// to find country specific information such as:
  - What countries are on the national threat list
  - What countries have high crime/type
  - Shots required
  - Visa/Passport requirements, etc…

Export Compliance – A Critical Requirement for ISSI

- Foreign sales is the fastest growing component of ISSI's commercial product success.
- In 2015, commercial sales were responsible for 7% of ISSI revenue and 30% of profit.
- 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.**

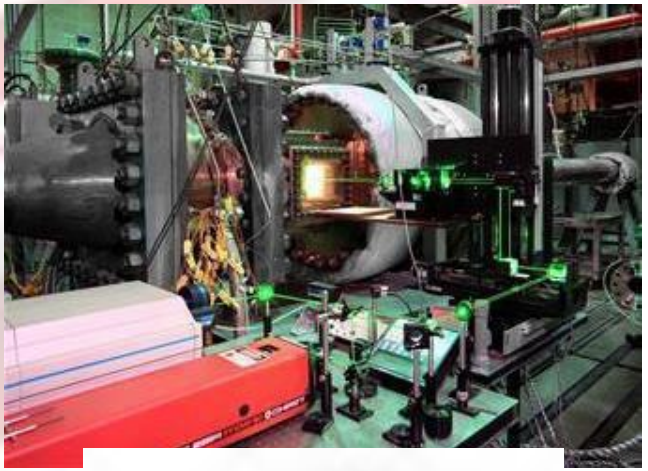
A Broad Range of Items are Subject to Export Controls…

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.

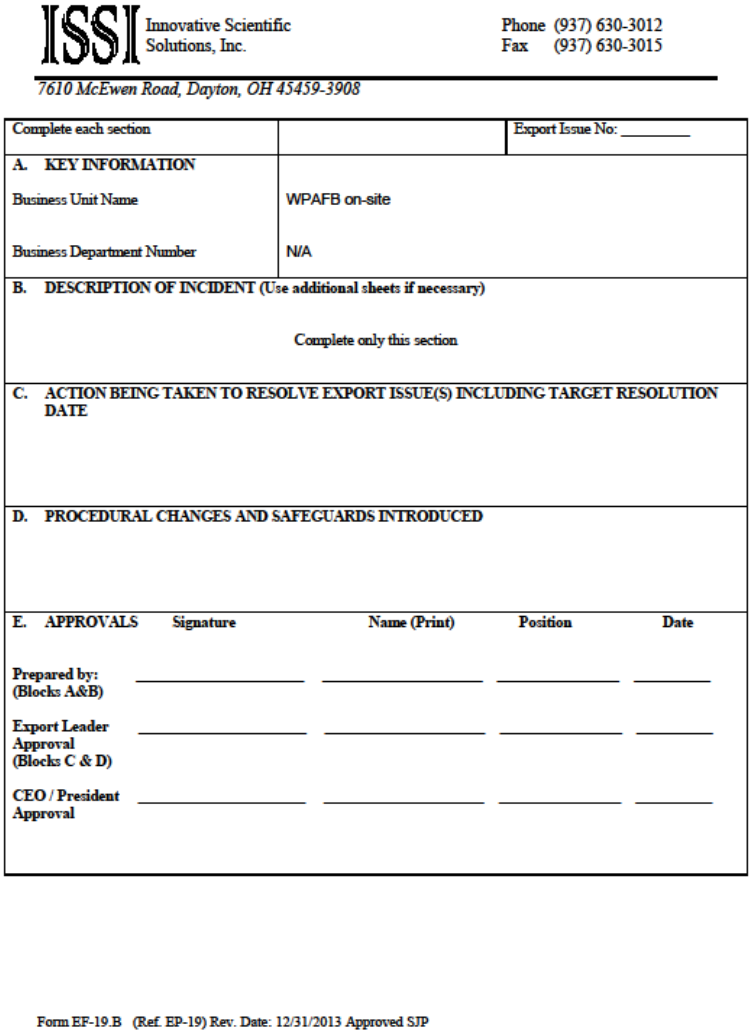


Organizational Responsibilities

- ***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:_____