DCSA CDSE Training Product Development and Maintenance

eLearning Student Guide
for
Counter-proliferation and Export Administration for FSOs
Product #: CI118

March 10, 2021

Developed For

Center for Development of Security Excellence

CDSE *training*

Developed By

Technologies

www.C2TI.com

11815 Fountain Way, Suite 200 Newport News, VA 23606

Contract Number: FY17F0012 ITSS Number: 1D10170007001

This page intentionally left blank.

Contents

Version Description Table

Version	Date	Remarks
Draft	January 2, 2020	Draft provided for CDSE review and comment
Final	March 24, 2020	Final provided for CDSE review and acceptance
V1.0		Source files

Color-coding is used as indicated below to highlight areas requiring CDSE SME input and to distinguish changes made from Draft to Final:

- Draft Delivery: Yellow highlighting indicates incomplete/missing content needed from the CDSE SMEs
- Final Delivery: Cyan highlighting indicates changes incorporated from CDSE SME feedback to draft documents/storyboards. If the C^2 development team makes any changes, not specifically requested by CDSE SMEs.

This page intentionally left blank.

Counter-proliferation and Export Administration for FSOs

Lesson: Course Introduction

Course Introduction Video (1 of 20)

John: The criminal investigation that stretched across four continents ended with a man in federal custody accused of smuggling and money laundering. Federal agents nabbed the man at Hartsfield-Jackson International Airport and that's where Channel 2's investigative reporter Jodie Fleischer is live with the exclusive details on the arrest. Jodie.

Jodie: Well, John, that man was flying from Paris to Panama, but he didn't know that his meeting was scheduled with an undercover federal agent; and, when he landed here in Atlanta for his stop-over, agents from Immigration Customs Enforcement and the Department of Defense were here to greet him.

Unnamed Person 1: It can be used in a wide variety of things. It can be used to enhance their military operations. It can be used to steal from U.S. industry.

Unnamed Person 2: High-tech gadgets so important to the United States Government, they're on a prohibited list—meaning you need special permission to export them out of the country—including radios, sensitive military encryption gear, and a controller for secure satellite communications for military aircraft, some of it developed by our National Security Agency.

Unnamed Person 1: Oftentimes, components are purchased so that specific technology can be reviewed, copied, or re-engineered for other purposes.

Unnamed Person 2: When agents caught Chi Tong Kuok at Atlanta's International Airport terminal, he [Chi Tong Kuok] told them he'd been acting at the direction of officials for the People's Republic of China and that they sought the items to figure out ways to listen to, or monitor, U.S. Government and military communications.

Course Introduction Video (Continued) (2 of 20)

Narrator: Export violations are a serious matter. Whether caused by willful misconduct, malfeasance, oversight, or other causes, the results can be catastrophic. The repercussions for these violations are equally serious. In fiscal year 2017, the Bureau of Industry and Security (BIS) investigations led to the criminal convictions of 31 individuals and businesses for export violations with penalties of over 287 million dollars in criminal fines, more than 166 million dollars in forfeitures, and 576 months of imprisonment. In addition, the Office of Export Enforcement, or OEE, and BIS's Office of Chief Counsel completed 52 administrative export matters, resulting in over 692 million dollars in civil penalties.

Conference Call (3 of 20)

Boss: Hello, everyone! I just want to say how proud I am of our facility security officer, or FSO, John Kent, who took action to prevent the illegal export of one of our technologies and reported suspicious activity to our government partners that resulted in an arrest! This was a direct result of our FSO learning the rules and regulations associated with export control and appropriately reporting suspicious activities.

Insert message: "Let's go back and identify how the FSO learned about these rules and regulations, and his responsibility to recognize and report suspicious activity."

Two months earlier…

Course Objectives Conference Call Follow-up (4 of 20)

Boss: Good afternoon, JK. Our company is bound by export control regulations and is frequently a target of foreign intelligence entities attempting to illegally acquire our technologies. I need you to learn everything you can about counter-proliferation and identify the government organizations that can help us.

Narrator: John Kent, better known as JK, is an FSO working in a cleared defense contractor facility. He leads an exciting life safeguarding critical technologies and protecting national security. But today he will take a break from this life of intrigue. His mission is to gain mastery over the topic of export control. Prior to beginning the task, JK is briefed on the objectives.

Course Objectives (5 of 20)

Boss: JK, here are your objectives for this mission. You must apply export control safeguards in order to determine if an export is allowed. According to the objectives, this means you will be able to describe counter-proliferation, recognize partnering organizations, recognize policy that governs counter-proliferation efforts, demonstrate an understanding of export permission guidelines, and explain the steps used to prevent and report export control violations. JK, you have been an FSO for more than three years, so I expect you to seek clarification wherever you may need it. There will be a briefing on this topic on the ninth floor. Several federal agencies will be coming to explain the talking points. Counter-proliferation has been a hot topic lately, and you're likely to come across folks discussing it on your way up. They may be able to provide background information about counter-proliferation.

Lesson: What is Counter-proliferation?

Counter-proliferation Basics (6 of 20)

Boss: JK is trying to understand what counter-proliferation is all about. On his way to the ninth floor he notices three colleagues who have been at the company longer than him, heading to the same floor. Help JK get the learning process started by finding out what the colleagues know about counter-proliferation. First, begin with learning the basics by understanding the definition,

purpose, and history of counter-proliferation.

Definition:

- Counter-proliferation is an effort to combat an excess of weapons, including weapons of mass destruction, long-range missiles, and certain conventional weapons.

Purpose:

- The U.S. Department of Commerce Bureau of Industry and Security (BIS) administers and enforces export controls on dual-use and certain munitions items through Export Administration Regulations (EAR) under the authority of the International Emergency Economic Powers Act (IEEPA).

History:

- Enforcement at BIS has evolved over the past 30 years into a sophisticated law enforcement agency, with criminal investigators and enforcement analysts who are singularly focused on export enforcement and work closely with licensing officers within a single bureau of the government. Using its subject matter expertise in the area of export controls, coupled with its unique administrative enforcement tools, export enforcement leverages relationships with partner law enforcement agencies and industry to maximize its impact.

Counter-proliferation Basics (7 of 20)

Boss: Now that JK has learned the definition, purpose, and history of counter-proliferation, he is ready to move on. Check the information board on the ninth floor to learn more.

Lesson: Partnering Organizations

Partnering Organizations (8 of 20)

Boss: Hey JK, how are things going?

JK: Great, I'm just looking at the partnering organization documents.

Boss: Let's go to my office, I'll explain them to you. Counter-proliferation involves efforts to combat the spread or growth of weapons — conventional weapons, weapons of mass destruction, and related technology — that threaten the United States. Several U.S. Government agencies — including law enforcement, licensing, and intelligence entities — are involved to restrict the sale and theft of restricted U.S. technologies to foreign nations, terrorist organizations, and others who might do harm to our country. The FBI, U.S. Departments of State, Commerce, Homeland Security, Treasury, Defense, and Energy play a critical role in export control activities both within the United States and outside its borders. We will discuss the personnel responsible for export control avoidance. Export enforcement has three program offices: The Office of Export Enforcement, or OEE, the Office of Enforcement Analysis, or OEA, and the Office of Antiboycott Compliance, or OAC. Export Enforcement blends the unique talents of its program offices to channel enforcement efforts against current and emerging threats to national security. Let's learn more about the roles played by some of these partnering organizations as well as the

Defense Counterintelligence and Security Agency, or DCSA.

Select each building to learn more about each partnering organization.

Office of Export Enforcement (OEE)

- The OEE is the only federal agency exclusively dedicated to the enforcement of export control law. This singular focus allows for development of requisite subject matter expertise to effectively enforce a complex regulatory regime. The OEE maintains Special Agents at offices across the United States, including its headquarters in Washington, D.C., and field offices located in:
    - Boston
    - Chicago
    - Dallas
    - Los Angeles
    - Miami
    - New York
    - San Jose
    - Houston (resident office)

Office of Antiboycott Compliance (OAC)

- The OAC administers and enforces antiboycott provisions of the EAR. OAC uses a threefold approach to carry out its mandate:
    - Monitoring boycott requests received by U.S. businesses
    - Levying enforcement actions when necessary
    - Guiding U.S. businesses to the particular transactions of the EAR
- In addition to these traditional compliance tools, OAC liaises with foreign governments to eliminate boycott requests at their origin. By working with U.S. Government partners in the Office of the U.S. Trade Representative and Department of State, OAC has met with officials of boycotting countries issuing boycott-related requests.

Office of Enforcement Analysis (OEA)

- The OEA supports the identification, prevention, investigation and prosecution of illegal exports, re-exports, and transfer of items subject to EAR. They do this by:
    - Analyzing the bona fides of foreign transaction parties to license applications (i.e., their reliability as recipients of U.S.-origin items)
    - Monitoring end-use and end-users of U.S.-origin exports
    - Identifying suspicious inquiries to alert U.S. companies
    - Developing investigative leads
    - Providing analytical case support
    - Engagement with key trading partners
- OEA accomplishes this mission through its Strategic Intelligence Division, International Operations Division, Export Control Officer Program, and Investigative Analysis Division.

Defense Counterintelligence and Security Agency (DCSA)

- The DCSA strengthens national security at home and abroad through oversight and education. DCSA oversees professional risk management services of U.S. and foreign classified information under the National Industrial Security Program (NISPOM). DCSA can act as a liaison between cleared industry and other federal partner organizations. Any indication of illicit proliferation of defense materials must be reported to DCSA under NISPOM 1-301 and 1-302b.

Partnering Organizations (9 of 20)

Boss: At this point, you have learned the definition, purpose, and history of counter-proliferation, as well as the partnering organizations that enhance export control efforts.

Lesson: Bureau of Industry and Security (BIS) Policy Guidance

Bureau of Industry and Security (BIS) Policy Guidance (10 of 20)

Boss: I have pulled the Bureau of Industry and Security, or BIS, Policy Guidance files for you to review before you leave. You can review the files outside my office on your way out. Give them to my assistant when you have completed your review.

JK: Thanks!

Narrator: There are several policies applicable to export control violations. Let's look at each of them.

Bureau of Industry and Security Administered Lists

Narrator: The Department of Commerce maintains screening lists, which advise the exporting public that listed persons are subject to specific end-user restrictions. In the event an entity, company, or individual on one of the following lists appears to match a potential party in an export transaction, additional due diligence to ensure the transaction does not violate the EAR is required before proceeding. These lists are available on the Government's Consolidated Screening List, which is on the BIS website. Select each list to learn more:

Denied Persons List

- Contains the names and addresses of persons subject to a denial of export privileges. Communications with a person on this list are prohibited.

Entity List

- Prohibits listed foreign persons from receiving some or all items subject to the EAR unless the exporter secures a license. Those on the Entity List were placed there because of the risk they pose of diversion of U.S.-origin items to weapons of mass destruction (WMD) programs, destabilizing accumulations of conventional weapons, terrorism, or other activities contrary to U.S. national security or foreign policy interests.

Unverified List (UVL)

- Contains the names and addresses of foreign persons that have been party to transactions subject to the EAR, whose bona fides could not be confirmed as a result of an end-use check, including the U.S. Government's inability to conduct such end-use check. A person listed on the UVL must meet three requirements:
    1. All export transactions must be reported in the Automated Export System (AES).
    2. License exception-eligibility is suspended.
    3. For all other EAR transactions not subject to a license requirement, the exporter must obtain a statement from the UVL party agreeing to abide by the EAR, including to permit an end-use check prior to export.

Consolidated Screening List

- The Consolidated Screening List (CSL) is a list of parties for which the United States Government maintains restrictions on certain exports, re-exports, and transfers of items.

Criminal and Civil Penalties

Narrator: In cases where there has been a willful violation of the Export Administration Regulations, or EAR, violators may be subject to criminal fines and administrative penalties. Administrative penalties may also be imposed when there is no willful intent, which means that administrative cases can be brought under a much wider variety of circumstances than criminal cases.

Previous Violation 1

- Company A, located in the United Arab Emirates, employed a network to illegally procure EAR99 U.S.-origin, dual-use, and military components for entities in Iran. Such components ended up in improvised explosive devices (IEDs) used against Coalition Forces in Iraq and Afghanistan. Company A's network is spread across several countries, including the United States. U.S.-origin goods diverted to Iran via this network include those controlled by the EAR for missile technology, national security, and anti-terrorism reasons, as well as those controlled under the International Traffic in Arms Regulations (ITAR). This case resulted from an investigation led by BIS's Miami Field Office with the assistance of U.S. Immigration and Customs Enforcement (ICE) and Defense Criminal Investigative Service (DCIS).

Select here to see the penalty

- On September 17, 2008, 75 additions were made to the BIS Entity List because of its involvement in a global procurement network which began with Company A. The Entity List prohibits Company A-related companies from receiving any items subject to the EAR unless the exporter secures a BIS license. On October 27, 2010, the Special Agent-In-Charge and three Special Agents of the Miami Field

Office received the Attorney General's Award for Excellence in Furthering the Interests of U.S. National Security for their efforts in leading this investigation.

Previous Violation 2

- Company B and Company C (both located in Hong Kong), and Company D, Company E, Company F, and Company G (all located overseas) engaged in actions contrary to the national security and foreign policy interests of the United States. These companies purchased EAR99 electronic components from the foreign subsidiaries of U.S. firms, and resold the components to persons in Iran and Iraq. These same components were later found in Iraq in unexploded IEDs and related materials. This case resulted from a joint investigation conducted by BIS's Los Angeles Field Office and the FBI.

Select here to see the penalty

- On July 20, 2011, all six companies were added to the BIS Entity List.

Previous Violation 3

- Company H worked with others to ship EAR99 industrial parts and goods, including a liquid/air separator, flame detector, motion sensor, pressure transmitter, circuit board, valves, connectors, and other miscellaneous parts, through Germany, Turkey and the United Arab Emirates to various petrochemical companies in Iran. In the course of this scheme, Company H also wired money to the United States, including over $300,000 sent to a bank account in Manhattan. On September 26, 2012, Company H's CEO pled guilty in Manhattan's federal court to conspiring to illegally export parts and goods designed for use in industrial operations from the U.S. to Iran. This case resulted from an investigation conducted by BIS's New York Field Office.

Select here to see the penalty

- On February 13, 2013, Company H's CEO was sentenced in U.S. District Court in the Southern District of New York to 12 months in prison.

<u>Voluntary Self Disclosures</u>

Narrator: Export Enforcement at BIS encourages the submission of Voluntary Self-Disclosures, or VSDs, by parties who believe they may have violated the EAR. VSDs are a compelling indicator of a party's intent to comply with U.S. export control requirements.

Select here for more

- Parties can submit an initial disclosure when any violation is first uncovered and follow-up with a complete narrative within 180 days. BIS carefully reviews VSDs received from disclosing parties to determine if violations of the EAR occurred and determine appropriate corrective action. Most VSDs are resolved with the issuance of a warning letter. Should Export Enforcement determine that issuance

of an administrative penalty is appropriate for the resolution of a VSD, authority is accorded to the VSD in assessing and mitigating the penalty. In some cases, fines and other administrative penalties may be significantly reduced and/or suspended for a probationary period.

Denial Export Privileges

Narrator: The BIS has the authority and discretion to deny all export privileges of a domestic or foreign individual or company under the EAR. Consider the potentially catastrophic impact upon a person or organization not being able to export, re-export, or receive any item — including an EAR99, which is the classification for an item that is subject to the EAR.

Select here for more

- BIS may impose a denial of export privileges as a sanction in an administrative case, or as a result of a person's criminal conviction under certain statutes. A denial of export privileges prohibits a person from participating in any transaction subject to the EAR. Furthermore, it is unlawful for other businesses and individuals to participate in an export transaction subject to the EAR with a denied person.

Asset Forfeiture

Narrator: Asset forfeitures target the financial motivation underlying many illicit export activities. The forfeiture of assets obtained in the conduct of unlawful activity may be imposed in connection with a criminal conviction for export violations, in addition to other penalties. Asset forfeitures prevent export violators from benefiting from their crimes, and with no statutory maximum, the value of forfeited assets can greatly exceed criminal fines or civil penalties.

False Statements

Narrator: A party to an export transaction may be subject to criminal and/or administrative sanctions for making false statements to the U.S. Government in connection with an activity subject to the EAR. Most frequently, false statements are made on an export document or to a federal law enforcement officer.

Bureau of Industry and Security (BIS) Policy Guidance (Continued) (11 of 20)

JK: Here are the folders back, thank you.

Terry (Assistant): Great! At this point, you should know counter-proliferation basics, partnering organizations, and have a better understanding of BIS policy guidance.
Screen text:

Boss: JK, it's almost time for my briefing on guidelines for exporting protected technology. The local DCSA CI Special Agent and IS Rep have arranged for this to happen soon. Want to walk with me?

JK: Sure.

Lesson: Permission Guidelines

Permission Guidelines (12 of 20)

Narration: Take a seat and observe what is being discussed.
Screen text:

Boss: Thank you all for coming today. I will be facilitating a discussion about guidelines for exporting protected technology. Some folks may be more educated about this than others, which is ok. We can learn from each other and make this a collaborative effort. To help everyone get acquainted, our speakers today include Jerry, the CI Rep from DCSA; Stephanie, the industrial security rep from DCSA; Paula, the CI Special Agent from DCSA; Steve, from the FBI; Kendra, from ICE; and Ron, from the legal department. Talking points are outlined in the handout in front of you. We'll proceed through this process by explaining each of the six areas.

Responsible Parties (Jerry) 1 of 1

Boss: Let's hear from our DCSA Counterintelligence Rep, Jerry.

Jerry: All parties that participate in transactions subject to the EAR must comply with the EAR. This could include any participants in an export transaction, such as exporters, freight forwarders, freight carriers, and consignees. The EAR applies to parties within the United States and in foreign countries.

Transshipment and Re-exports (Stephanie) 1 of 1

Boss: Let's hear from our DCSA Industrial Security Rep, Stephanie.

Stephanie: Parties to an export transaction cannot bypass the EAR by shipping items through a third country. Transshipment or re-export of items in international commerce may be a violation of U.S. law. Parties to exports or re-exports of items subject to the EAR should be alert to red flag indicators of possible unlawful diversion (found in Supplement Number 3 to Part 732 of the EAR) and should follow BIS guidance.

"Catch-all" (Paula) 1 of 1

Boss: Let's hear from our DCSA CI Special Agent, Paula.

Paula: The BIS controls exports of items based on their technical specifications, intended end-use, and the end-user. The EAR imposes license requirements on exports of items if the exporter knows or has reason to know that any of the items will be used in a manner or by an entity that may cause particular concern to the U.S. Government. These licensing controls are often referred to as "catch-all" controls because they apply to a broad set of items, or in the case of WMD activities, to any item subject to the EAR, even if the item wouldn't ordinarily require a license based on its technical specifications.

Successor Liability (Steve) 1 of 1

Boss: Let's hear from our FBI Agent, Steve.

Steve: Businesses should be aware that the principles of successor liability may apply. They should perform due diligence in scrutinizing export control practices of any company they plan to acquire. A properly structured due diligence review can determine if an acquired company has violated export law. This review should examine export history and compliance practices, including commodity classifications, technology exchanges, export licenses and authorizations, end-users, end-uses, international contracts, the status of certain foreign employees who have access to controlled technologies, and the company's export policies, procedures, and compliance manuals.

Educational Outreach (Kendra) 1 of 1

Boss: Let's hear from our representative from ICE, Kendra.

Kendra: To raise awareness of export control requirements and prevent potential violations of the EAR, Export Enforcement conducts educational outreach to U.S. exporters and foreign trade groups. In addition to participating in BIS export control seminars and conferences, Export Enforcement conducts outreach to individual exporters to inform them of their responsibilities under the EAR and review compliance best practices, and alert them if appropriate, of offshore illicit procurement activities of which they may be a target. Export Enforcement also engages American business communities overseas as well as foreign trade and industry associations.

Cyber-Intrusions and Data (Ron) 1 of 1

Boss: Let's hear from our legal perspective representative, Ron.

Ron: A new area of focus in our outreach effort relates to cyber-intrusions and data exfiltration that can result in your export-controlled technology ending up overseas. It is becoming an almost daily occurrence to read about a cyber-intrusion or attack. Former President Obama identified cyber threats as "one of the most serious economic and national security challenges we face as a nation." The perpetrators of illicit cyber-crime are varied; they include independent hackers, criminal organizations, and state actors. The theft of export-controlled information from computer systems as a result of foreign cyber actors is a threat to U.S. national security interests and your company's competitive lifeblood: intellectual property.

Permission Guidelines (13 of 20)

Boss: Thank you for attending this briefing; I hope you were able to gain a better understanding of exporting guidelines. Our company has an export control supervisor, Lisa, who works with our security personnel, legal counsel, and sales team to ensure we comply with the guidelines. JK, please report to Lisa to gain additional knowledge on the steps used to prevent and report export control violations.

Narrator: At this point JK should have a better understanding of the definition, purpose, and history of counter-proliferation, partnering organizations, BIS policy guidance, and permission guidelines.

Lesson: Export Control Compliance

Export Control Violations (14 of 20)

Lisa: John Kent, great to see you, come on in! I've been expecting you. I know that you have been exposed to the counter-proliferation basics, policy, and permission guidelines. Now I'm going to give you some insight into the elements of an effective export compliance program. There are several elements that fit together to make up an effective export compliance program. These elements do not necessarily constitute an exhaustive list. BIS weighs a variety of aggravating and mitigating factors in deciding the level of penalties to assess. As set forth in Supplements 1 and 2 to Part 766 of the EAR, having an effective export compliance program is strongly considered when assessing penalties. BIS's Export Compliance Program (or ECP) guidelines can be accessed through the BIS website under the Compliance and Training tab.

Export Compliance Program (ECP) Guidelines (15 of 20)

Lisa: BIS employs the following eight guiding elements when assessing the effectiveness of a company's export compliance program:

(Audits) The export compliance program and its parts must be regularly tested and recalibrated for validation. Functional level audits focus on specific areas of the export process, such as record-keeping or shipping procedures, whereas program level audits at the corporate level look at the ECP in its entirety.

(Record Keeping) The record-keeping requirements in Part 762 of the EAR describe how long to keep records, what type of records are required, how to reproduce documents, and which documents are exempted from retention. You should create a system to manage records that includes good operational security measures, such as securing the data and properly disposing of media with export information.

(Training) When designing a training program, make the message as specific as possible to the target audience. This will help the staff understand their role, their responsibilities, and their contributions to the ECP.

(Export Authorization) The goal of this element is to build procedures and processes to guide correct export decisions. This includes knowing which agency's jurisdiction over the export confirms the export classification control number, determining what license is required for the end destination, and the most critical aspect, screening. Screening all parties to the export transaction is essential for ensuring that export-controlled items do not fall into the wrong hands.

(Export Violations and Corrective Actions) Procedures and clear guidance must be given to all employees that lists actions to take in suspected incidents of export-related noncompliance. This involves detecting noncompliance, taking early mitigation actions, garnering senior management support, and establishing an environment free from reprisal. Voluntary self-disclosure of export noncompliance and taking corrective actions will be a mitigating factor in determining Export Enforcement administrative action.

(Management Commitment) Every effective ECP uses a top-down process, with the organization's senior management adding significance and legitimacy by publicly supporting compliance policies and procedures and creating a management commitment statement, providing sufficient resources, and supporting export compliance training for all staff.

(Risk Assessment) Risk is a function of threat, vulnerability, and impact. Common risks include the unauthorized release of sensitive information or technology, ineffective organization operations such as a weak compliance structure, and the potential threat from unknown end-users or end-uses of the export control item.

(Build and maintain your Export Compliance Manual) An effective ECP benefits the company by protecting against unintended export violations, threats to the company's intellectual property, and fines or other losses.
Tailor the export compliance manual to meet the company's needs, and remember, it's a living document — update it regularly!

JK: Thanks for showing me the completed puzzle.

Export Compliance Program (ECP) Guidelines (Continued) (16 of 20)

JK: I have a question. Can you more specifically explain what ITAR and EAR administration is about? I just want to make sure I have a concrete understanding of the two.

Narrator: Select the ITAR and EAR button to continue.

ITAR and EAR (17 of 20)

Lisa: International Traffic in Arms Regulations, or ITAR, and the Export Administration Regulations, or EAR, are export control regulations run by different departments of the U.S. Government. Both are designed to help ensure that defense-related technology does not get into the wrong hands. Export license is a general term for ITAR- and EAR-controlled items in which the U.S. Government has granted permission to transport or sell potentially dangerous items to

foreign countries or parties. The following agencies play a role in administering U.S. export controls via the ITAR and EAR.

U.S. Department of Commerce BIS

- Administers and enforces export controls on dual-use and certain munitions items for the Department of Commerce through the EAR under the authority of the International Emergency Economic Powers Act (IEEPA).

Department of State

- Controls the export of defense articles and services subject to the ITAR

Department of Energy

- Controls exports and re-exports of technology related to the production of special nuclear materials

Nuclear Regulatory Commission

- Controls the export of certain nuclear materials and equipment

Department of the Treasury

- Administers economic sanctions programs

Defense Counterintelligence and Security Agency

- May take appropriate action in the case of exports involving classified technical data or defense articles to ensure compliance with the DoD National Industrial Security Program Operating Manual (NISPOM)

Export Compliance Program (ECP) Guidelines (Continued) (18 of 20)

Lisa: The last thing I have for you today are the steps to obtain an export license. The steps to obtain a license are not too complex or tough to understand. As a reminder, whether or not a license is required depends on the item being exported. The item's export control classification number, or ECCN, will identify the need for a license. The ECCN is a five-character alpha-numeric designation used on the commerce control list, or CCL, to identify dual-use items for export control purposes. I will give you an overview of the necessary steps to take in the event a license is needed. Getting an export license: visit the BIS site; select the licensing tab; select 'SNAP-R register' to complete an application to ensure you're eligible to apply for licensing. At this point you should receive an ID number via email. Now you may apply for the license. Once applied for, it could take 30–40 days to receive your license in the mail. If you need assistance to determine whether the item you want to export requires a license, you should check the BIS website or call one of our export counselors for assistance. Please note that whether you are the exporter, freight forwarder, consignee, or other party to the transaction, you must address any red flags that arise.

JK: Thank you for all your help.

Lisa: No problem. In the real world, you will be presented with businesses that may not be up to par on export standards, so all this information is important.

Export Compliance Program (ECP) Guidelines (Continued) (19 of 20)

Lisa: Before you go, I want to show you some resources that I will forward to you. Here you go. The BIS website resource includes the export control office, export counselors, access to penalty guidelines, control lists, information about ITAR and EAR, getting an export license, and the U.S. consolidated screening list.

JK: Thanks. I am heading to my office now. I will be sure to download all the resources.

Lesson: Course Conclusion

Course Conclusion (20 of 20)

Boss: JK, do you have everything you need to cover counter-proliferation cases?

JK: I believe so.

Boss: Now that you've completed this training, you should be able to describe counter-proliferation, recognize partnering organizations, recognize policy that governs counter-proliferation efforts, demonstrate an understanding of export permission guidelines, and explain the steps used to prevent and report export control violations. Great job!

Reminder: Counter-proliferation resources can be accessed from the course resources screen.

Scenario 1: Introduction (1 of 14)

Boss: Soon I'll be forwarding you a transaction that was flagged in our system. I need you to check it out after you log on to your computer.

Scenario 1: Email (2 of 20)

Narrator: Help JK answer the challenge question so that he can access his computer.

What is the definition of counter-proliferation?

- Department of Defense effort to combat proliferation of legal drugs
- Department of Defense effort to combat proliferation of thieves
- Department of Defense effort to combat proliferation of weapons

Scenario 1: Email (3 of 20)

Narrator: JK thinks this email looks a bit suspicious.

From: John Smith

To: John Kent

Subject: Export business proposal

Message:

Hello, my name is John Smith from the mid-western region of the world. I have been conducting business with many parts of the world for years. After taking over my family business, I am seeking to expand more in the United States. I am inquiring about purchasing 400 replica weapons.

Part of what I do is train people to become familiar with firearms, along with various other things. I am planning to use the weapons for training purposes only. I will not need any manuals. I am familiar with many weapons and have an idea of how they all operate. I plan to pay cash for the items, and extra if this can be expedited in a quick fashion. I would really appreciate it if you decide to conduct business with me.

Best,

JS

Narrator: JK knows that "400 replica weapons," "mid-western region," and "paying cash" are rare requests and red flags.

Scenario 1: Resources (4 of 20)

Narrator: Now that you have found the red flags, to whom are you obligated to report them?

Question: Which two BIS resource links are appropriate for reporting red flags?

- Export control office
- Access to penalty guidelines
- Control lists
- Export counselors
- Information about ITAR & EAR
- Getting an export license

Scenario 1: License Requirements (5 of 20)

Narrator: Good job. Figure out what else needs to be done.

Question: What must Assi Industries do first in order to figure out if a license is required?

- Check the ECCN
- Check the ITAR List
- Check the Business License Number

Narrator: Assi Industries should first check the ECCN. The ECCN is a five-character alpha-numeric designation used on the CCL to identify dual-use items for export control purposes.

Scenario 1: E-mail Response (6 of 20)

From: Boss
To: Johnathan Kent
Subject: Red Flags
Message:

Hey JK, we have found some disturbing news as we followed up on the red flags you reported today.

Our records notified us of the sender's alias name used in previous business interactions. Do not bring attention to the matter as one of our partnering organizations will take things from here.

Thank you for reporting those red flags; it made a huge difference in understanding whether or not this was a legit business deal. Thank you!

Best,

Boss

Question: Which of the following are the partnering organizations?

- Office of Export Enforcement (OEE)
- Office of Antiboycott Compliance (OAC)
- Office of the Security Manager (OSM)
- Office of Enforcement Analysis (OEA)
- Defense Counterintelligence and Security Agency (DCSA)

Scenario 1: Summary (7 of 20)

Narrator: Good job, JK! You've helped the agency thwart another enemy! Soon, he'll have another task.

Scenario 2: Introduction (8 of 20)

Boss: Good afternoon JK. I have an assignment for you. There is a small business in our supply chain that's not up to par on counter-proliferation guidelines, and I would like for you to help them get on the right track.

JK: Sure thing! I'll head over to the facility to talk with the owner.

Scenario 2: Business Store (9 of 20)

JK: Hello, how are you today?

Business owner: I'm doing alright, how can I help you?

JK: Well, as part of our company's supply chain, we like to ensure you are following counter-proliferation rules and regulations. This is a procedure we do for new businesses.

Business owner: Ok, sure.

JK: Thank you for your time. To begin, I would like to know your method of delivering electronic parts to various customers outside the U.S.

Business owner: I have a first come, first served method. Whoever requests parts will get them upon payment and stock amount. However, I haven't had to conduct international business yet.

Scenario 2: Consolidated Screening Lists (10 of 20)

JK: Hmm, there are a few steps you are missing, but this is why we visit folks in our supply chain and get them caught up to the exporting standard. When shipping an item to another country, you must first check the end-user.

Scenario 2: Knowledge Check: Consolidated Screening Lists (11 of 20)

Narrative: Choose the resource where JK can find information about checking the end-user to show the business owner.

Answer to question:

1. Select resources
2. Select Consolidated Screening Lists

Scenario 2: Red Flags (12 of 20)

Business Owner: Ok, this makes sense. Is there more to this process?

JK: Yes, next you want to find out the proposed use of your delivered parts. This should be clearly indicated with the initial request for parts. However, if it's not, this is considered a red flag and you must report them to…

Scenario 2: Red Flags (Continued) (13 of 20)

Answer to question:

1. Select resources
2. Select BIS site

Question: Which three BIS resources links are appropriate for reporting red flags?

- Export control office
- Access to penalty guidelines
- Control lists
- Export counselors
- Information about ITAR & EAR
- Red flag indicator

Scenario 2: Export License (14 of 20)

Business owner: Oh ok, I'm following. However, why would I need an export license to ship items to another country? I was planning to use a third-party company to handle that.

JK: Export licenses are required on specific items. Export license is a general term for both ITAR- and EAR-controlled items in which the U.S. Government has granted permission to transport or sell potentially dangerous items to foreign countries or parties.
To decide if your items require an export license, you must first look up its ECCN number. This can be found using the …

Scenario 2: Knowledge Check: Export License (15 of 20)

Answer to question:

1. Select resources
2. Select BIS Website

Question: Which BIS resource link is appropriate for looking up an ECCN?

- Commerce Control List (CCL)
- Access to penalty guidelines
- Enforcement

Scenario 2: ECCN (16 of 20)

JK: You begin by searching for your item on the CCL Index. When you find a potential ECCN, read through the ECCN entry before determining if your item fits into the parameters of that ECCN.

Business owner: Ahhhhh, that makes a lot of sense.

JK: Yes, so once you have checked end-uses and end-user, verify the need for an export license, and keep your staff up to date about the process and handling of future orders.
If your item requires an export license, just go to the license resource page and it will prompt you. This can be found at…

Scenario 2: Knowledge Check: ECCN (17 of 20)

Answer to question:

1. Select resources
2. Select BIS Website

Question: Which two BIS resource links are appropriate to get an export license?

- Regulations
- Access to penalty guidelines
- Control lists
- Licensing
- Information about ITAR & EAR
- Application

Scenario 2: Penalty Guidelines (18 of 20)

Business owner: Sure thing! How can I find out the penalties for anyone who doesn't comply? You know that information is good for training.

JK: Sure thing. You can find it right here…

Scenario 2: Penalty Guidelines (19 of 20)

Answer to question:

1. Select resources
2. Select BIS Website

Question: Which three BIS resource links are appropriate for locating penalty guidelines?

- Export control office
- Enforcement
- Penalties guidelines
- Export counselors
- Information about ITAR & EAR
- Office of Export Enforcement (OEE)

Scenario 2: Summary (20 of 20)

JK: That's all I have for you today. I'll email you the resources. Any further questions or concerns should be directed to the BIS site, which will be your primary source of information regarding export control.

Business Owner: Thank you, I appreciate the information. Thanks to you, I now know the importance of knowing the end-use and end-user, understanding when an export license is needed, the International Traffic in Arms Regulations, and Export Administration Regulations.

Narrator*:* JK has clearly mastered the topic of counter-proliferation and he is ready to resume his life of intrigue as an FSO.