# FOCI OUTSIDE DIRECTORS, PROXY HOLDERS, AND VOTING TRUSTEES TRAINING (IS183.16-IS188.16)

This training consists of six modules and is specifically designed for the Defense Security Service's Outside Director (OD), Proxy Holder (PH) and Voting Trustee (VT) community. ODs, PHs and VTs play an important role in the effective implementation of Foreign Ownership, Control, and Influence (FOCI) Mitigation Agreements. They are responsible for performing their duties in a manner believed to be in the best interests of the company but consistent with the national security concerns of the United States.

# Student Guide

## FOCI Outside Director- Proxy Holder Training

### Course Information

| | |
|---|---|
| **Purpose** | These courses are specifically designed to assist the Outside Director (OD), Proxy Holder (PH), and Voting Trustee (VT) to understand their critical roles and responsibilities at Foreign Ownership, Control, or Influence (FOCI) mitigated companies. |
| **Audience** | Defense Security Service's OD, PH, and VT community |

### FOCI ODs, PHs, VTs

Welcome to the Foreign Ownership, Control, or Influence (commonly referred to as FOCI) Outside Directors, Proxy Holders, and Voting Trustees Training (collectively referred to from this point on as “Outside Directors”).

As an Outside Director, you play a critical role in the success of your company’s industrial security program. You are expected to represent the national security interest of the United States. Your primary responsibility is to help ensure that the cleared company under FOCI Mitigation Agreement implements all needed procedures and organizational changes pertaining to the security and safeguarding of classified and export controlled information.

This training is covered over 6 Modules.

### Modules 1–6

- Module 1 (IS183.16) provides an introduction to DSS, FOCI and the FOCI Mitigation Agreements.
- Module 2 (IS184.16) discusses Managing FOCI Mitigation and its Affiliates.
- Module 3 (IS185.16) discusses the Role and Responsibilities of the Government Security Committee (GSC).
- Module 4 (IS186.16) will discuss some responsibilities unique to the Proxy Holder and Voting Trustee.
- Module 5 (IS187.16) discusses the Security Vulnerability Assessment (SVA) and Best Practices.
- Module 6 (IS188.16) discusses what is expected during the Initial Meeting, the Annual Compliance Report, and the Annual Meetings.

# Student Guide

## FOCI Outside Director- Proxy Holder Training

### Module 1 (IS183.16) - Introduction to DSS, FOCI, and FOCI Mitigating Agreements

#### *1.1 Module 1: Introduction*

Introduction to DSS and Foreign Ownership, Control, or Influence. Commonly known as FOCI.

Let's begin with the objectives of Module 1.

#### *1.2 Module 1: Objectives*

In this Module, you will be given an introduction to Defense Security Service (or DSS). You will be given the definition of FOCI and an overview of the FOCI Factors that DSS considers in the aggregate to determine how to best mitigate the FOCI.

You will be given a description of the FOCI Lifecycle followed by the FOCI Mitigation Instruments DSS uses to protect the classified and export-controlled information from the foreign entities.

#### *1.3 DSS Overview*

The Under Secretary of Defense for Intelligence provides authority, direction, and control over Defense Security Service.
DSS is an agency of the Department of Defense (DoD) headquartered in Quantico, Virginia with field offices throughout the United States.
DSS provides the military services, defense agencies, over 28 Federal agencies, and approximately 13,500 cleared contractor facilities with security support services.
DSS is a unique organization, partnering with both industry and government stakeholders. DSS is in effect the face of government to industry and represents the government interests to industry. The DSS mission is to oversee the protection of U.S. and foreign classified information and technologies in the hands of Industry and serves as the functional manager for the DoD security professional development program.

#### *1.4 FOCI Definition*

According to the National Industrial Security Program Operating Manual (NISPOM), "A U.S. company is considered to be under FOCI when a foreign interest has power, direct or indirect, whether or not exercised, to direct or decide matters affecting the management or operations of the company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts."

Refer to Course Resources link, Module 1.

#### *1.5 FOCI Factors*

FOCI factors are considered in the aggregate to determine whether a company is under FOCI. DSS will analyze the factors to determine if there is FOCI and what the appropriate level of protection measures are needed to mitigate or negate the foreign risks and foreign interests at the applicant Company.

Before FOCI Factors can be analyzed, they must be identified accurately and understood within the context of the organization's need for a Facility Security Clearance (FCL).

### *1.6 FOCI Factors*

DSS considers the following questions during the Analysis, the Mitigation, and the Adjudication phases:

Q1: Are there any known foreign risks that would jeopardize the classified programs or contracts?

### *1.7 FOCI Factor Q2*

Has the company previously demonstrated willingness to place controlled technologies at risk?

### *1.8 FOCI Factor Q3*

What information, assets, or resources required protection from foreign risk or control?

### *1.9 FOCI Factor Q4*

What level of foreign influence or control is involved and how does it impact the company's business operations, decisions, and ability to act independently from the foreign stakeholder(s)?

### *1.10 FOCI Factor Q5*

Does the company operate a legitimate, lawful business in general, not just for technology transfer?

### *1.11 FOCI Factor Q6*

Are there industrial security agreements, declarations of principles, or other formal understandings in place with the foreign country?

### *1.12 FOCI Factor Q7*

Is your company subject to foreign government influence or control, and to what extent?

### *1.13 FOCI Factor Q8*

Are there any other factors that indicate or demonstrate a capability on the part of the foreign interests to control or influence the operations or management of the business organization concerned?

### *1.14 FOCI Lifecycle*

The FOCI process has five phases:

1. Identification and Assessment
2. Mitigation Negotiation
3. Mitigation Implementation
4. Mitigation Oversight, and

5. Change Condition, Amendment, or Renewal.

### *1.15 Identification & Assessment*

In the first phase, **Identification and Assessment,** the source of the FOCI is identified through the review of forms and documents provided by the company and open sources.

The process begins with the company submitting the SF 328, "The Certificate Pertaining to Foreign Interest" which is submitted by the Company's Facility Security Officer (FSO) into the Electronic Facility Clearance System (e-FCL).

The SF 328 is a 10 question document designed to help identify the presence of FOCI in a Company.

Refer to the Course Resources link, Module 1.

### *1.16 Mitigation Negotiation*

In the second phase, **Mitigation Negotiation,** DSS analyzes the information and determines what actions are necessary to address the FOCI.

DSS decides the action plan that must be taken to prevent unauthorized access to classified information.  DSS reviews and negotiates the draft plan with the company.

Once the agreement is decided upon, DSS will request the nomination of Outside Directors based on the type of agreement.

### *1.17 ECP Definition*

**The Electronic Communication Plan (ECP)** is a requirement for FOCI mitigated companies to ensure effective oversight by the Government Security Committee (GSC) of electronic communications and networks between the cleared company and its Affiliates.

The GSC establishes written policies and procedures assuring electronic communication between the FOCI Company and its subsidiaries and the Affiliates do not disclose classified information or export controlled information without proper authorization.  ECP ensures that the Affiliates cannot exert influence or control over the FOCI Company's business or management in a manner that could adversely affect the performance of classified contracts.

### *1.18 AOP Definition*

**The Affiliated Operations Plan (AOP)** is a requirement for FOCI mitigated companies when they enter into operational relationships with their Affiliates.

Business functions or teaming arrangements with affiliates of a FOCI mitigated company are not authorized unless approved by the Government Security Committee or GSC (GSC will be discussed later) and DSS in advance.  Instances when DSS identifies an affiliated service occurring without approval may negatively impact a company's Security Rating.

DSS has developed a template AOP to assist industry in requesting DSS review.

### *1.19 FLP Definition*

**Facilities Location Plan (FLP)** is a requirement when a FOCI mitigated company is located within the proximity of a foreign parent or an Affiliate that would reasonably inhibit the cleared company's ability to comply with the FOCI agreement. Such scenarios may include being located in the same building, campus, or adjoined buildings with an Affiliate.

FOCI collocation is not authorized, and DSS will determine when a company is collocated in its sole discretion. When a company is located within close proximity to its foreign parent or an affiliate a FLP must be approved by DSS in advance.

### *1.20 Visitation Plan Definition*

**The Visitation Plan** is a requirement for FOCI mitigated companies to ensure visitation with the Affiliates is controlled as required by the FOCI mitigation agreement.

The FOCI Mitigation Agreements (SCA, SSA, Proxy, and VT) establish requirements for visitation between the FOCI Company and their Affiliates. Any deviations from the requirements in the FOCI mitigation agreements must be approved prior to implementation by DSS.

### *1.21 Mitigation Oversight*

In phase four, **Mitigation Oversight,** the Annual Compliance Report is prepared and the Annual Meeting is conducted by DSS with the company, the Outside Directors, and the Affiliates.

During this phase the Annual Security Vulnerability Assessment (SVA) is conducted by the field office and Headquarters personnel.

This will be covered in Module 5.

### *1.22 TCP Definition*

**The Technology Control Plan (TCP)** is a facility specific requirement for FOCI mitigated companies to outline how they will provide protection to classified and export controlled information.

The TCP establishes measures to assure that access by non-U.S. citizens and the foreign affiliates is strictly limited to only the information for which appropriate Federal Government disclosure authorization has been obtained. This plan is approved by DSS and shall be developed and implemented by those companies cleared under a Voting Trust Agreement (VTA), Proxy Agreement (PA), Special Security Agreement (SSA), or Security Control Agreement (SCA).

DSS may also require a TCP be developed in other situations in its sole discretion.

Refer to the Course Resources link, Module 1.

### *1.23 Mitigation Implementation*

In the third phase, the **Mitigation Implementation** process is where the final approvals for the selected mitigation instrument are finalized, signed by the company, and DSS.

This includes the following Mitigation Implementation Plans which may be included during the mitigation negotiation process: the Electronic Communication Plan (ECP), the Technology Control Plan (TCP), the Affiliated Operations Plan (AOP) and the Facilities Location Plan (FLP).

In this phase the Outside Directors are approved and the scheduling of the initial meeting will take place (the initial meeting will be discussed in Module 5).

When a company operates under any of the FOCI Mitigation Agreements as a Voting Trust, Proxy, Special Security, or Security Control Agreement they may be required to develop additional procedures to ensure their FOCI is effectively mitigated. This is where these plans come into the picture.

### *1.24 Change Condition*

The last phase is the **Change Condition, Amendment, or Renewal of the agreement**.

This phase is a result of any changes, amendments, and/or renewal of the existing Agreement.

### *1.25 Mitigation Instruments*

There are two basic types or categories of Mitigation Instruments. They include the Minority Ownership/Control and the Majority Ownership/Control. These FOCI Mitigation Instruments are designed to provide a general overview and will vary on content based on the needs of each business entity.

### *1.26 Minority Ownership*

**The Minority Ownership/Control** category involves companies in which the foreign interest does not effectively own or control the company, but has a beneficial stake of five percent or more in the cleared company. Minority foreign ownership is usually mitigated with a Board Resolution (BR) or a Security Control Agreement (SCA), unless the foreign stakeholder has additional control that requires more stringent mitigation, such as veto power over the board decisions.

**Board Resolution:**

A BR is a legally binding acknowledgement passed by the company's Board of Directors. The BR formally acknowledges the foreign investors and excludes them from access to classified or export controlled information and has no involvement in the classified programs. The foreign shareholder does not sit on the board nor has the right to appoint a member to the board. The BR also formally acknowledges any indebtedness the Company has with a foreign entity.

**Security Control Agreement:**

A SCA preserves the foreign owner's voice in the business management of the company while denying unauthorized access to classified and export controlled information. The foreign entity does not effectively own or control the cleared U.S. Company, but it is entitled to representation on the Board. If the foreign shareholder sits on the Board of Directors or has the right to appoint a representative, an SCA, along with at least one Outside Director is usually sufficient to mitigate the FOCI.

For samples of each of these Agreements refer to the Course Resources link, Module 1.

### *1.27 Majority Ownership*

**Majority Ownership/Control** involves foreign interest that has direct or indirect majority ownership, or effective control, over the cleared U.S. company(s). The mitigation instruments used to mitigate the FOCI includes the Special Security Agreement, or known as an SSA, a Proxy Agreement or known as a PA, or a Voting Trust Agreement, known as a VTA.

**Special Security Agreement:**

An SSA is an agreement imposing various industrial security measures denying unauthorized access to classified and export controlled information while preserving the foreign owner's voice in the business management of the company. If the classified contracts require access to proscribed information a National Interest Determination may be required.

**Proxy Agreement:**

A PA is an agreement whereby the foreign owner relinquishes most rights associated with ownership of the company by conveying voting rights to the proxy holders, who must be cleared U.S. citizens approved by the U.S. Government.

**Voting Trust Agreement:**

A VTA is similar in effect to the PA, except under a VTA the foreign owner transfers legal title in the company to the cleared U.S. citizen ("Trustees") approved by the U.S. Government.

For samples of each of these Agreements refer to the Course Resources link, Module 1.

### *1.28 Module 1: Conclusion*

You have completed Module 1, which provided you with an overview of DSS, definition of FOCI, a review of the FOCI factors, the FOCI lifecycle, and an explanation of the mitigation instruments.

# FOCI Outside Director- Proxy Holder Training

## Module 2 (IS184.16) - Administering the FOCI Agreement and Compliance

### *2.1 Module 2: Introduction*

Welcome to Module 2, Administrating the Foreign Ownership Control or Influence (FOCI) Agreement and Compliance by the Company, its parent company, and the Affiliates.

This module supports the Outside Directors, Proxy Holders, and the Voting Trustees to identify the types of business structures and their corporate governance documents and their role as a board member.

Now that the FOCI Action Plan is in place and the company's governing board of directors have been established, each party of the FOCI Agreement is entrusted to abide by the provisions in that agreement and agree to ensure unauthorized access of any classified and export controlled information by the foreign parent or affiliates.

Let's take a look at the objectives for this module.

### *2.2 Module 2: Objectives*

The objective includes an overview of the basic business structure which includes the organization chart, governance documents, and governance body. We will familiarize you with the role of the Senior Management Official (SMO) and the Inside Director.

We will briefly go over the two committees known as the Government Security Committee (GSC) and the Compensation Committee. We will discuss the qualification, appointment, and removal of the Outside Directors, Proxy Holders, and the Voting Trustees. We'll explain the operations of the FOCI Agreement, best efforts and the board's relationship with the Affiliates.

Let's start with the business structure and why it is important.

### *2.3 Basic Business Structures*

Understanding the basic business structure of your company and its corporate governance documents is critical to your position as a board member. Whether your company is a Privately or Publicly Held Corporation, Limited Liability Company (LLC), Limited or General Partnership you should review the governance documents to understand your role on the board.

Typically, the business structure includes an organization chart, the governance documents such as Articles of Incorporation or Certificate of Formation, By-laws, Operating Agreements, Shareholders Agreement and Business License.

Once the FOCI agreement is put in place, the Articles of Incorporation and the By-Laws should be changed or a meeting minute executed to establish the new corporate board to include the Outside Directors as members. If applicable, the Senior Management Official and the Inside Director should be identified as well.

We covered the basic business structure now let's talk about the organizational chart.

Refer to the Course Resources link, Module 2.

### *2.4 Organizational Chart*

Business structures can be complex and may even involve more than one foreign entity in the chain of ownership or investments.  It is important that you understand your Corporate Organizational Chart. The chart identifies all Affiliates (other companies owned by the foreign parent company) in the chain of ownership and any companies that fall under the requirements of the FOCI Mitigation Agreement, such as any cleared subsidiaries.

***Remember, the FOCI Agreement applies to the entire corporation, not just the cleared employees.***

The Organizational Chart should also identify the associations between the cleared facilities and the ultimate parents to include percentages of ownership, Facility Security Clearance (FCL) status, "Commercial and Government Entity" (CAGE) codes and other helpful information explaining the relationship among the companies in the chain of ownership.  It is also useful to educate employees of the company under FOCI and their interactions with the foreign parent and the affiliates.

Now let's take a look at Corporate Governance Documents.

Refer to the Course Resources link, Module 2.

### *2.5 Corporate Governance Document*

As a board member it is important to recognize the company's business strategies and how to integrate the security measures of the FOCI Mitigations Agreement.

This involves becoming familiar with the Company's day-to-day operation.

### *2.6 Corporation Documents*

Let's talk about what corporate documents:

The basic governance documents for a Corporation include:

- Articles of Incorporation
- Corporate By-Laws
- Loan agreements
- Shareholder Agreements (if applicable)
- Purchase Agreements
- Corporate Stock Ledger indicating stockholders name(s)
- Overall percentage(s) of ownership, and
- The most recent copy of Board Meeting minutes

Other governance documents that may require reviewing are:  Letters of Intent, Partnership or Joint venture Agreements, Licensing and/or patent agreements, the company's financial reports, and operating agreements.

### *2.7 General Partnership Documents*

In the case of an LLC and Limited or General Partnership the governance documents could include:

- Articles of Organization
- Operating Agreement
- Membership list with member/manager name(s), and
- Overall percentage(s) of capital commitment

### *2.8 Limited Partnership Documents*

When the company is a Limited Partnership the Corporate Governance documents would include:

- Certificate of Limited Partnership
- Partnership Agreement
- Partnership list with limited/general partner name(s), and
- Overall percentage of capital commitment.

Special attention should be placed on any foreign indebtedness or company's purchases of foreign subsidiaries, and how dependent the company is on the foreign entities or shareholders. These documents should be consistent with the FOCI Agreement.

Good corporate governance includes transparency for corporations and investors, sound disclosure policies, and communication beyond disclosure through dialogue and engagement as necessary and appropriate.

Companies must achieve the right balance between the appointment of independent and non-independent directors to ensure boards have an appropriate range and mix of expertise, diversity, and knowledge.

### *2.9 Governing Body*

The FOCI Company's governing body should ensure that reporting requirements to the Shareholder(s) are met. These reports should not circumvent the governing body's responsibilities as the controlling entity for the FOCI Company.

The governing body manages the performance reviews of the SMO and other company Senior Executives (as determined by the Compensation Committee), not the foreign parent or Affiliates.

It is important to familiarize yourself with the management of the company's business and the composition of the governing body or Board of Directors for both your company and all the Affiliates in the chain of ownership. This should include the Chief Financial Officer (CFO), Inside Counsel, and the President of the company.

As Outside Directors, Proxy Holders, and the Voting Trustees, you share all the same rights, powers, privileges, immunities, and duties as members of the board in decision making of the company business and security matters.

When a company(s) is operating under a Special Security Agreement (also known as an SSA) or Security Control Agreement (SCA) the Affiliate's participations is limited to the position of the Inside Director(s).

Companies operating under Proxy or Voting Trust Agreements are expected to exercise all management prerogatives to ensure the FOCI Company is organized, structured, and financed.

The FOCI Company should be capable of operating as a viable business entity independent from its foreign parent company and its Affiliates.

### *2.10 Senior Management Officials*

The Senior Management Official (SMO) is one of the Corporate Key Management Personnel (KMP). Examples of a SMO include such positions as the Chief Executive Officer (CEO) or the President.

The SMO shall be subordinate to the FOCI Company's governing body and ***shall not report directly to the foreign parent or to the affiliates*****.** The day-to-day operation of the FOCI Company resides with the SMO.

DSS expects the FOCI Company's governing body to manage the reporting requirements to the Shareholder. This may be achieved by establishing the format and process for the FOCI Company to report to the Shareholder.

### *2.11 Inside Director*

The Inside Director is a representative of the foreign affiliate from the parent company.

The Inside Director serves as one of the Board of Directors and is also a permanent committee board member on the Compensation Committee only for the SSA or the SCA.

Companies operating under an SSA or SCA authorize the Affiliates to have representation on the governing body of the Company through the position of an Inside Director(s).

- An Inside Director shall ***NOT*****:**
- Be the Chairman of the Board
- Have access to classified or export controlled information held by the FOCI Company (except as permissible under applicable U.S. law)
- Take any action to direct or decide matters affecting the operations of the FOCI Company that may result in unauthorized access to classified information
- Adversely affect the performance of contracts which have access to classified information, or
- Undermine the U.S. national interest due to unauthorized access to critical U.S. technology

Please note that the Proxy Agreements and the Voting Trust Agreements do not have Inside Directors.

# FOCI Outside Director- Proxy Holder Training

We just discussed the Inside Director's role. Now we will discuss the two different committees starting with the GSC.

### *2.12 Government Security Committee*

The GSC is a permanent committee of the Corporation Board, consisting of the Outside Directors and other Directors who are also officers of the Corporation and who have personnel security clearances.

Members of the GSC shall exercise their **"Best Efforts"** to ensure the compliance measures are implemented pertaining to security and safeguarding of classified and export controlled information.

### *2.13 Compensation Committee*

The Compensation Committee is established and required in the SSA, SCA, and FOCI Mitigation Agreements. It is a permanent committee consisting of at least one Outside Director and one Inside Director.

The Committee is responsible for recommending the annual compensation of the Corporation's Company Principals, who are the management personnel spelled out in the company's charter documents, to the Corporation's Board for approval.

In the Voting Trust Agreement, the Compensation Committee consists of three Trustee Directors elected by the Board of Directors. They decide which officers or other visitors to invite to the committee.

The committee has the authority to determine compensation for the Chief Executive Officers and other Executives.

The committee will have the sole authority to set, amend, or terminate corporate goals and objectives of the CEO.

### *2.14 ODs, PHs, & VTs*

On the Board of Directors, the number of Outside Directors should equal or exceed the number of Inside Directors for an SCA and must exceed the number of Inside Directors for an SSA. (Inside Directors are not allowed in a Proxy Agreement or Voting Trust Agreement.) As an Outside Director (Proxy Holder/Voting Trustee), you are expected to represent the national security interests of the United States and exercise all the rights, powers, and responsibilities as a Board member, imposed by applicable statutes, regulations, and the Corporation's charter and by-laws.

When you were nominated by your company to serve as an Outside Director the following criteria applies as long as you hold that position. You:

Must be a resident U.S. citizen

Must be capable of exercising management prerogatives which ensure that the foreign owner/entity can be effectively insulated from the company.

Must be a totally disinterested individual capable of exercising judgment independent of any influence(s) that might prejudice your decision making capability.

Must assure that you have no potential conflicts of interest or business relationships with any other positions/boards that you may hold or serve.

Must/continue be eligible for a personnel security clearance at the level of the facility's clearance level.

Next we will discuss the procedures for adding, replacing, or removing the Outside Directors, Proxy Holders and the Voting Trustees.

***2.15 ODs, PHs, & VTs***

The Outside Directors, Proxy Holders, and Voting Trustees are responsible for the effective implementation of the Foreign Ownership Control Influence (FOCI) Mitigation Agreement.

Their responsibilities are:

- Abiding by and enforcing the FOCI Agreement in place
- Ensure the Facility Security Officer, Directors, and employees comply with the provisions of the Facility's Mitigation Agreement
- Attend the Quarterly Board and Government Security Committee (GSC) meetings
- Emplace a Technology Control Plan, Electronic Communications Plan, and Visitation Procedures
- Ensure there are no Affiliate Services* being provided between the FOCI Company and the Affiliates that have not been approved in advance by the GSC and DSS
- For instances with potential FOCI Collocation, develop and submit a Facilities Location Plan for DSS review and approval
- Maintain oversight to ensure all Affiliated services, FLPs, TCP, ECPs, and Visitation Procedures are fully implemented and effectively mitigate the FOCI
- Ensure that DSS (through the DSS Rep) is advised of any known attempts to violate any provision of the Facility's mitigation agreement or relevant U.S. government contract provisions related to security, U.S. export control laws, or the NISP
- Communicate any material changes to the DSS
- Required to serve on the GSC

The GSC's responsibilities will be covered in detail in Module Three.  In addition to these responsibilities the Proxy Holders and Voting Trustees have other requirements outlined in their Proxy Agreement and Voting Trust Agreement that are unique.

* Affiliated Services may also be called Affiliated Operations.

### *2.16 Adding Replacing or Removing*

There are situations when Outside Directors, Proxy Holders, and Voting Trustees are removed or resign from their position. Other times a company may add additional Outside Directors, Proxy Holders, and Voting Trustees due to a possible change in the business structure. In the event of the death, resignation, removal or inability to act of any Outside Directors, Proxy Holders, and Voting Trustees the Company should give prompt written notice to DSS and the Shareholder.

The Outside Directors, Proxy Holders, and Voting Trustees may not be removed without a written notice stating no objection from DSS. For special cases the corporation can *immediately* remove an Outside Director, Proxy Holder, and Voting Trustee to prevent possible damage to the corporation or violations to statue and regulations. DSS can be notified prior to or concurrently of this type of removal.

Here are some other common reasons for removal:

- Any reason permitted by the provisions of applicable state laws or the company's certificate of incorporation or by-laws
- Violations of the FOCI Agreement, or Inability to protect the legitimate economic interest of the shareholder.

### *2.17 Adding Replacing or Removing*

Appointments of new and/or the replacement of Outside Directors, Proxy Holders, and Voting Trustees, should not become final without the approval by DSS.

In the case of an SCA/SSA, if the company's shareholders removed the Outside Director, the successor is nominated by the Company. In the event of a vacancy, the Parent Corporation fills the vacancy.

In the case of the Proxy Agreement or Voting Trust Agreement the remaining Proxy Holder or Voting Trustee shall nominate a successor and notify the shareholders and DSS of the nominee.

As the sole stockholder, the Parent Corporation may remove an Outside Director, Proxy Holder, and Voting Trustee.

In the case of an SCA/SSA, the shareholder(s) can remove the Outside Director.

The Outside Director position must not be vacant more than 90 days.

### *2.18 Operations of the FOCI Agreement*

The key to the success of a FOCI company is the result of collaboration between management and the Outside Directors, Proxy Holders and Voting Trustees. Together they implement policies and practices through the GSC to ensure the safeguarding of classified and controlled unclassified information, to include the performance of the classified contracts or programs.

This is accomplished by putting security measures in place at the company such as:

Technology Control Plan (TCP)

Electronic Communications Plan (ECP)

Affiliated Operations Plan (AOP)

Facility Location Plans (FLP)

The GSC should also establish policies and procedures for the Visitation Policy and work closely with the FSO to ensure that all of the above plans and policies are effective.

### *2.19 "Best Efforts"*

What should Best Efforts mean to you as a board member?

Your actions should reflect:

(1) honesty in belief or purpose,

(2) faithfulness to one's duty or obligation,

(3) observance of reasonable standards of fair dealing

### *2.20 "Best Efforts"*

To Achieve "Best Efforts" means "Performing your duties reasonably and in a manner to believe to be in the best interests of the Corporation but consistent with the national security concerns of the United States."

"Best Efforts" Definition:

Performing your duties, including fiduciary duties, in good faith and in a manner believed to be: (i) in the U.S. national interest; (ii) where not consistent with the national interest, in the best interest of the Company and the Company's shareholders in accordance with applicable state law to the extent that any such state law is not preempted by this Agreement; and (iii) with such care, including reasonable inquiry, as an ordinarily prudent person in a like position would use under similar circumstances.

### *2.21 "Best Efforts"*

The FOCI Company should be structured in such a way that it is not dependent upon the foreign parent to meet performance requirements on classified contracts.

The foreign parent should not circumvent the FOCI Company's governing body with regards to the operations of the FOCI Company.

As a member of the Board you should establish your relationship with the foreign parent in the areas of:

- Commercial & Non-commercial
- Financial Reporting to foreign parent and the Affiliates

- Role of the Inside Director, Outside Directors, Proxy Holders & Voting Trustees in relationship to foreign parent and the Affiliates

### *2.22 Module 2: Conclusion*

You have completed Module 2, on Administrating the FOCI Agreement and Compliance by the Company and its parent company and Affiliates which covered the:

- Business Structures
- Senior Management Official
- Inside Director
- Government Security Committee and Compensation Committee
- Qualification of Outside Directors and Removal or Replacement of an Outside Directors
- Operations of the Provisions of the FOCI Agreement
- "Best Efforts"
- Relationship with the parent company and Affiliates

### Module 3 (IS185.16) - Roles and Responsibilities of the Government Security Committee (GSC)

#### *3.1 Module 3: Introduction*

In Module 3, we cover one of the most important committees you will serve on as an Outside Director, Proxy Holder, and Voting Trustee that is the Government Security Committee (GSC). As previously stated, the FOCI company is required to establish a permanent committee of its Board of Directors and the Outside Directors, known as the GSC.

The formulation of this special executive-level security committee is very significant in overseeing matters that affect the performance of classified contracts.

DSS looks to the GSC to maintain policies and procedures to ensure the company complies with U.S. export control laws and regulations and safeguards classified information entrusted to the company.

The GSC also ensures that the company complies with the DoD Security Agreement (DD Form 441, which is the Agreement between the government and the company on security measures) and appropriate security provisions and compliance program of the Agreement.

Let's take a look at the objectives for this module.

#### *3.2 Module 3: Objectives*

The objectives for this module are:

- Explaining the structure of the GSC
- Identify the responsibilities of the GSC performance standards
- Describe and identify the Development and Implementation of the Compliance programs and Policy, which consist of:
    - Technology Control Plan (TCP)
    - Electronic Communication Plan (ECP)
    - Affiliated Operations Plan (AOP)
    - Facilities Location Plan (FLP)
    - Visitation Policies
- Discuss the Quarterly Meetings
- Discuss the Closed Sessions for classified, Export Control, and/or controlled unclassified information
- Describe how to prepare the Financial Reports to the foreign parent

Let's begin with the structure of the GSC.

#### *3.3 Structure of GSC*

The role of the GSC is to ensure that the Company maintains policies and procedures to safeguard classified information and export controlled information in the possession of the Company and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

The GSC should also ensure that the Company complies with U.S. export control laws and regulation and does not take action deemed adverse to performance on classified contracts.

The GSC consists of all cleared Outside Directors, Proxy Holders and Voting Trustees and all cleared officers/directors (if any).

### *3.4 GSC Chairman*

The structure of the GSC includes:

The Chairman is an Outside Director designated by the GSC and has responsibilities that include:

- Designate a Secretary
- Provide advice and consent in selecting and retaining the Facility Security Officer (FSO) and the Technology Control Officer (TCO)
- Prepares the Annual Implementation and Compliance Report along with the CEO

### *3.5 GSC Secretary*

The Secretary, who must be a member of the GSC, has responsibilities that include:

- Ensuring that all records, journals and minutes of GSC meetings are kept.
- Prepare and retain other documents sent to or received by the GSC and made available for inspection by DSS.

### *3.6 Technology Control Officer*

The TCO is also appointed by the company as the principal advisor to the GSC concerning the protection of Export Controlled Information and administering the TCP.

### *3.7 Facility Security Officer*

The company appoints the FSO, who is not a member of the GSC, but is the principal advisor to the GSC concerning the safeguarding of classified information.
Therefore, it is not permitted for the company to remove the FSO/TCO without the advice and consent of the Chairman of the GSC.

### *3.8 GSC Performance Standards*

The members of the GSC, the FSO, and the TCO must exercise their “Best Efforts” to ensure that all provisions of the Agreement are carried out and complied with by the Company’s management, employees, the foreign parent, and its Affiliates.

### *3.9 GSC 2*

They should also advise DSS of any known violation of, or known attempt to violate any provision of the Agreement or contract program provisions regarding security, U.S. export control laws and regulations and the NISPOM.

### *3.10 GSC 3*

This also includes the GSC's exercise of appropriate oversight and monitoring of the Company's operations to ensure that the protective measures contained in this Agreement are effectively maintained and implemented.

### *3.11 GSC 4*

The FSO plays an important role in the operational oversight of the Company's compliance with the requirements of the NISPOM and advises the GSC appropriately.

### *3.12 GSC 5*

Any discussions of classified information and/or export controlled information by the GSC must be held in closed sessions and minutes of the meetings must be recorded and safeguarded in accordance to the security requirements.

### *3.13 GSC 6*

The GSC, FSO, and TCO must be available to brief the DSS representative on their responsibilities and the NISPOM, U.S. export control laws and regulations and the FOCI Agreement.

### *3.14 GSC 7*

Each member of the GSC must execute and submit to DSS, upon accepting the appointment and thereafter at each annual meeting, a certificate that acknowledges:
1) The protective security measures taken by the Company to implement this Agreement; and
2) The U.S. Government has placed its reliance on him or her as a U.S. citizen and as the holder of a personnel security clearance to exercise his or her "Best Efforts" to ensure compliance with the terms of this Agreement and the NISPOM.
3) Each member of the GSC must further acknowledge his or her Agreement to be bound by and to accept his or her responsibilities under the Agreement.

### *3.15 GSC 9*

The GSC must oversee the foreign parent representative, known as the Inside Director, is compliant with the obligations mentioned in the Agreement.

The GSC has the authority to review, approve, and/or disapprove Visit Requests, according to the provisions of their specific Agreement, to the company by any personnel who represent any of the foreign parent and any of the Affiliates. This includes the directors, officers, and employees.

### *3.16 GSC 10*

The Chairman of the GSC should hold regular quarterly meetings with the GSC members. Representatives of the foreign parent and the company's management may be invited to attend.

At least one of the Outside Directors will attend all Company Board and Company

Board committee meetings in order for there to be a quorum.

The GSC must maintain a chronological file of all Visit Requests, reports of visits, and contact reports, together with appropriate approvals or disapprovals, which should be maintained by the GSC for review by DSS.

The GSC must submit the Implementation and Compliance Report to DSS.

### *3.17 Compliance Program & Policies*

The GSC must ensure the company develop and implement a detailed FOCI compliance program to include the following:

- Technology Control Plan (TCP)
- Electronic Control Plan (ECP)
- Affiliated Operations Plan (AOP)
- Facility Location Plan (FLP)

The GSC is required to develop and oversee the Visitation Policy/Procedures.

### *3.18 Technology Control Plan*

The purpose of the Technology Control Plan (TCP) is to preclude the possibility of inadvertent access by non-U.S. citizens/foreign nationals assigned to or employed by cleared Companies to information (unauthorized disclosure or export of Export Controlled Information consistent with applicable U.S. laws and regulations) for which they are not authorized.
The TCP describes all security measures and should address both the:

- Physical access (buildings, restricted areas, etc.) and
- Technical access (e.g., data networks, servers, etc.)
- Any disclosure of classified information to foreign persons in a visitor status or in the course of their employment by the cleared U.S. Company is considered an export disclosure under the International Traffic in Arms Regulations (ITAR).

Now let’s take a look at the Electronic Communication Plan.

For additional information on TCP see the Course Resources link, Module 3.

### *3.19 Electronic Communication Plan*

The purpose of the Electronic Communications Plan (ECP) requires maintaining policies and procedures enabling effective oversight of communication between Company personnel and the foreign owner and/or Affiliates to prevent their exertion, influence, or control over the Company’s business.

The GSC must ensure the Company takes the necessary action, and maintain oversight to provide assurance to itself and DSS that electronic communications between the company and its subsidiaries and the Affiliates do not disclose classified or Export Controlled Information without proper authorization.

There are different forms or types of communication, they include:

- Any means of data transfer, transmitted in whole or in part by wire, radio, cable, or other like connection
- By electromagnetic, photo-electronic, photo-optical, electronic, mechanical or other device or system (could also include data storage, or the Cloud)
- Videoconferences, Cell Phones, and Facsimile
- Internet, instant messaging (such as Lync and Gmail, Instagram, Twitter), and email
  Collaboration applications (such as: SharePoint and WebEx)
- Network connectivity/infrastructure, etc.

For additional information on ECP see the Course Resources link, Module 3.

### *3.20 Electronic Communication Plan*

The GSC must include the following in their ECP:

- Detailed network configuration diagram that clearly shows all communications networks and facilities used by the company for the transmission or storage of electronic communications, and
- It must delineate which networks will be shared and which should be protected from access
- Network descriptions addressing firewalls, physical and logical access controls, remote administration, monitoring, maintenance, retention, and the electrical and physical separation of systems and servers, as appropriate

Next we will look at the Affiliated Operations Plan (AOP).

For additional information on ECP see the Course Resources link for Module 3.

### *3.21 AOP*

The purpose of an AOP is to identify companies operating under a FOCI Mitigation Agreement who share administrative or other services from the foreign parent/Affiliates. The intent of the AOP is to provide DSS and the GSC with an understanding of the operational relationship between the FOCI Company and the foreign parent/Affiliates to ensure risks to the performance on classified contracts are effectively mitigated.

A company is consider under FOCI when they:

- Receives administrative or other services from an Affiliate
- Provides such services to an Affiliate
- Shares a third party service provider or employees with an Affiliates
- Commercial arrangements in the form of contracts and subcontracts, joint research, development, marketing or other types teaming arrangements with an Affiliate
- Affiliate technology products or services in performance on classified contracts

- Other shared services and products, which need prior approval from DSS before they can be added to the AOP

Typically these services are routine operations and do not relate directly to classified or export control work. Companies operating under a FOCI mitigation instrument must receive prior approval from the GSC and DSS before utilizing such service.

GSC members should know what cooperative endeavors are performed by the Company whether directly or through third-party service providers; shared employees, commercial arrangements, shared services and products, and Affiliate technology.

For additional information on AOP see the Course Resources link for Module 3.

### *3.22 AOP*

There may be circumstances when the parties to a merger or acquisition propose in the FOCI action plan that the U.S. Company provides certain services to the foreign interest, or the foreign interest provides services to the U.S. Company. The services to be provided must not violate the FOCI Mitigation Agreement and should be included by the AOP. DSS approves the services in the AOP before the Company can engage in the using the shared services.

The GSC will:

- Submit the AOP for DSS approval ensuring no unapproved operations are occurring at the FOCI Company, and that the FOCI Company notifies DSS of any proposed changes to an AOP prior to them occurring.
- Certify annually that the AOP is effectively executed and that the Affiliated Operations do not circumvent the requirements of the FOCI Mitigation Agreement.
- Will update and approve any substantive change made to an existing AOP and forward to DSS for final approval prior to implementing changes.

### *3.23 AOP Services*

Relationships with the Affiliates requiring advance approval include:

- Shared Third-Party Services
- Shared Employees or Persons
- Cooperative Commercial Arrangement
- Other Shared Services and Products
- Affiliate Technology

Shared Third-Party Services is a service provided by a third party to both the cleared Company, and any of its Controlled Entities, and Affiliates. This could include professional services such as accountant, legal, tax, information technology, or business consultant, as it complies with the Agreement.

Shared Employees/Person are Affiliate personnel assigned/employed to support work in whole or in part in support or on behalf of the Company or any Controlled entities

Company employees are assigned to work in support on behalf of any Affiliate.

Cooperative Commercial Arrangement includes commercial transactions in the form of contracts, subcontracts, joint research, development, marketing, or other type of teaming arrangement between the U.S. Company and any Affiliate. Both parties should not be subject to pressure or duress from the other party.

Other Shared Services and Products includes category of valuable products or services provided other than in a commercial company or any of its Controlled Entities to any Affiliate. Other Shared Services and Products are not permitted prior to DSS approval of a corresponding AOP.

Affiliate Technology is when the FOCI Company uses technology products or services of an Affiliate in performance on a contract requiring access to classified information. The company's management notifies the Government Contracting Activity (GCA), regarding the technology products or services under that contract. The company must include this notification as an addendum to the AOP. In the event that GCA elects not to receive notification, the company must include the GCA's written statement opting out of notification as an addendum to the AOP.

For additional information on AOP see the Course Resources link for Module 3.

### *3.24 AOP Risks*

**Affiliated Operations Risk Factors:**
Individuals performing service may have unauthorized access to classified or controlled unclassified information

Company does not provide the appearance of a separate entity from its Affiliates to DSS, its employees or its government customers

AOP results by DSS - mitigated with Proxy Agreement/Voting Trust is not a viable business entity

Cannot demonstrate ability to comply with all requirements FOCI agreement
The service(s) would:

- Allow a parent/Affiliate to exert undue control or influence over the company or employees
- Permit access by a parent/Affiliate to employee adverse information
- Permit access by a parent/Affiliate to customer accounts and data
- Threats to operational security is not in best interest of National Security

### *3.25 FLP*

The purpose of a Facility Location Plan (FLP) is the collocation concern when a FOCI-mitigated company is located within the proximity of the foreign parent or an Affiliate as defined within the FOCI Mitigation Agreement which would reasonable inhibits the company's ability to comply with the FOCI Agreement.

The Company must have written approval from DSS of a FLP prior to collocating. The company and the GSC must demonstrate to DSS that being closely located to an Affiliate does not affect the Company's ability to comply with its FOCI Mitigation Agreement.

**The FLP must:**

- Identify organizational relationship between collocated entities (parent, Affiliate, etc.)
- Create maps and floor plans showing where employees occupy space in each facility
- Describe the existing collocation situation & identify why the entities are collocated
- Identify if the arrangement is interim or permanent
- Identify common areas
- Demonstrate if effective separation of the facilities in the areas of IT systems, phone systems, access control systems, alarm systems or guards
- Establish mitigation measures to ensure full compliance with the FOCI Mitigation Agreement

### *3.26 FLP*

**The GSC is responsible for:**

- Overseeing the development and implementation of the FLP
- Submitting the FLP for DSS approval prior to the FOCI Company becoming located within close proximity to an Affiliate
- Monitoring the FLP to ensure all FOCI Mitigation requirements are met
- Ensuring the FOCI Company notifies DSS of any proposed changes to an FLP prior to them occurring
- Certifying annually that the FLP has been effectively implemented and being located in close proximity to an Affiliate has not degraded the Company's ability to comply with their FOCI Mitigation Agreement
- DSS identification of an unreported FOCI Collocation may negatively impact the status of the FOCI Company's Facility Security Clearance.

Lastly, let's look at the Visitation Policy.

For additional information on FLP see the Course Resources link for Module 3.

### *3.27 Visitation Plan*

The purpose of the Visitation Plan is to ensure visitation with the foreign parent/Affiliates are controlled as required by the FOCI mitigation Agreement.

Under the Visitation Policy the Agreement distinguishes the requests as "Visit" and "Routine Business Visits."

**Visit Requests are:**

All personnel who represent any of the foreign parent/Affiliates, including all the directors, officers, employees, representatives, and agents

Exception for Inside Director, if attending Company Board meetings or Company Board Committee meetings, do not need Visit Request

Meetings at any location within or outside of the United States to any facility owned or operated by foreign parent/Affiliates

At the discretion of the GSC, may also include certain videoconferences and teleconferences

**Approval of Visit Requests.**

All requests for visits must be submitted or communicated in advance through the FSO to the designated Outside Director for approval. The Visit Request should include:

- The exact purpose
- Justification
- List of attendees
- Location of the visit
- Date and time of the visit
- Minutes from the meeting

For additional information on a Visitation Policy see Course Resources link, Module 3.

***3.28 Visitation Plan***

**Approval of Routine Business Visit Requests.**

All requests for Routine Business Visits must be submitted or communicated in advance to the FSO for approval. The Routine Business Visit Request should include:

- Must state the basis of the visit
- Must include appropriate documents
- Date and time of the visit

The GSC, in its reasonable business discretion, may with the approval of DSS:

- Designate specific categories of Visit Requests other than those enumerated as Routine Business Visits not requiring the advance approval of the designated Outside Director
- Determine that, due to extraordinary circumstances involving the security of classified information and/or Export Controlled Information, certain types of Visits that might otherwise be considered Routine Business Visits are to be allowed only with the advance approval of the designated Outside Director.

For additional information on a Routine Visits see Course Resources link, Module 3.

***3.29 Visitation Plan***

**Routine Business Visits are:**

- Commercial aspects of the Company's business,
- Made in connection with the regular day-to-day business operations of the Company
- Discussion or reviewing commercial performance versus plans or budgets, inventory, accounts receivable, accounting and financial controls, implementation of business plans and technical development programs
- Commercial suppliers, solicitation of orders, quotation of prices, products and services on a commercial basis
- Financial, or legal matters necessary for compliance with the requirements of any foreign or domestic government, stocks, and securities
- Marketing and technical activities relating to import/export of products for compliance with regulations of U.S. Departments or Agencies, Department of Defense, Commerce, State, and Treasury

For additional information on a Routine Visits see Course Resources link, Module 3.

### *3.30 Visitation Plan*

**Routine Business Visits do not involve:**

- KMP,
- The transfer or receipt of classified information or
- Export Controlled Information, or
- Activities bearing upon the Company's performance of its classified contracts.

For additional information on a Routine Visits see Course Resources link, Module 3.

### *3.31 Visitation Plan*

The Outside Director, along with the FSO should also maintain a record of all Visit Requests, including both approved and/or disapproved and information regarding completed visits, such as the date, place, personnel involved, and summary of material discussions or communications. This record shall be maintained by the designated Outside Director and shall be periodically reviewed by the GSC and DSS.

For additional information on a Visitation Policy see the Course Resources link for Module 3.

### *3.32 Quarterly GSC Meetings*

The purpose of the quarterly meetings is to discuss the company business and any security matters. The Chairman of the GSC or Outside Directors shall provide, to the extent authorized by the Agreement, regular quarterly meetings of the GSC.

At the discretion of the GSC, representatives of the foreign parent/Affiliates and the Company's management personnel may also be invited to attend to the quarterly meeting. The Inside Director may be invited to the meeting.

Quarterly meeting discussions include anything concerning the compliance to the Agreement, issues, and actions concerning the company. The discussion could either be business or security related on topics such as:

- Sales of capital assets
- Business of the company
- Mergers
- Consolidation or reorganization of the company or its assets
- Business ventures
- New government contracts, and
- Any shareholder decisions including reviewing and/or formatting of financial reporting

The GSC is responsible for the maintenance of records together with appropriate approvals or disapprovals pursuant to this Agreement shall be maintained for review by DSS.

This includes a chronological file of all Visit Requests, reports of visits, and contact reports.

### *3.33 Financial Reports*

All FOCI Mitigation Agreements allow for the flow of financial information from the FOCI Company to the foreign parent in a manner that does not compromise classified information or may adversely affect the performance of classified contracts.

FOCI Companies can provide the foreign parent with the following financial information, which should be included in the report:

- financial statements
- budget forecasts
- independent financial audit reports
- financial information necessary to file consolidated tax returns
- information related to material investment or financing decisions, and
- other financial documents in accordance with the FOCI Mitigation Agreement

The format of the financial reporting is subject to approval by the GSC and should be reviewed at the quarterly GSC meetings. The FOCI Company should coordinate with the foreign parent/Affiliates on the format for financial reporting. Proxy Agreements require DSS approval of the financial report format.

### *3.34 Closed Sessions*

Closed Sessions are any discussions of classified information and/or Export Controlled Information by the GSC. These meetings or discussions must be held in closed sessions in accordance with applicable security requirements related to the classification level of the information discussed.

The minutes of such meetings shall be recorded and safeguarded in accordance with applicable information security requirements and made available ONLY to such authorized individuals as are so designated by the GSC.

### *3.35 Module 3: Conclusion*

You have completed Module 3, on Roles and Responsibilities of the Government Security Committee (GSC) which covered the:

- Structure of the GSC
- GSC performance standards
- FOCI Compliance Programs and Policy

Lastly, we discussed the role the GSC has in the quarterly meetings, financial reports, and closed sessions.

## Module 4 (IS186.16) - Additional Responsibilities of Proxy Holders and Voting Trustees

### *4.1 Module 4: Introduction*

In Module 4, we will discuss the Additional Responsibilities of the Proxy Holders and Voting Trustees; which includes their exclusive rights, powers, and authority to exercise all voting rights with respect to the shares of the corporation.

This is accomplished in a way that ensures that the foreign shareholder can be effectively insulated from the cleared company. Although the Proxy Holders and Voting Trustees have similar responsibilities, there are some differences that will be covered in this module.

### *4.2 Module 4: Objectives*

The objective of this module is:

- Identify difference between the Proxy Agreement and Voting Trust Agreement

We will discuss:

- Meetings with the shareholder(s)
- Approved visits and communications with the Affiliates and shareholders
- Accepting shares or dividends
- Voting discretion
- Compensation of Proxy Holders and Voting Trustees
- Annual Review and Certification

### *4.3 Proxy Holder and Voting Trust Agreements*

The Proxy Agreement and Voting Trust Agreement may be used when a cleared company is effectively owned or controlled by a foreign entity. The Proxy Agreement and the Voting Trust Agreement are substantially identical arrangements whereby the voting rights of the foreign owned stock are vested in cleared US citizens approved by the Federal Government (DSS). Neither arrangement imposes any restrictions on the company's ability to have access to classified information or to compete for classified contracts.

The difference between the Proxy Agreement and the Voting Trust Agreement is that under the Voting Trust Agreement the foreign owner transfers legal title in the company to the Trustees that are approved by DSS.

A company could use either a Proxy Agreement or a Voting Trust Agreement to mitigate the FOCI when the foreign parent is controlled by the foreign government OR if the government customer requests a stronger mitigation and requires access to proscribed information.

For further information regarding the Proxy Agreement or Voting Trust Agreement refers to the FOCI Agreement for your company or your DSS representative.

Refer to Course Resources link, Module 4.

### *4.4 Meetings with Shareholder(s)*

There are similarities that the Voting Trustees and the Proxy Holders share regarding meetings with their Shareholder(s).

They include:

- Schedule a meeting on a quarterly/annual basis
- Additional meetings may be scheduled to discuss financial condition and/or operation of the company
- Shareholder representatives may attend if requested by the Proxy Holders or the Voting Trustees
- Prior to meeting a written agenda should be prepared and submitted to DSS for approval
- Response is received from DSS of the approval prior to the meeting.
- Minutes of meetings in which Shareholder representatives are in attendance shall be prepared and retained by the GSC for review by DSS
- Classified and Export Controlled Information should not be disclosed to the Shareholder(s) except as specifically authorized by applicable law or regulation.
- Suggestions or requests by the Shareholder representatives present at these meetings should not be binding on the Proxy Holders/Voting Trustees or the Company.
- May convene a meeting with the Shareholder at any time as long as the agenda is limited to the matters described in the Proxy Agreement or Voting Trust Agreement

  In addition to the prior items listed, the Voting Trustees provide:
- A written agenda is completed in advance which include items requested by Shareholder for the Voting Trustees approval.
- Meetings with the parent company may convene at any time, without prior approval from DSS.
- Before voting the Shares, the Voting Trustees must obtain written consent of the Parent on any issue that may adversely affect an Investor.

### *4.5 Visits and Communication*

The Proxy Agreement and Voting Trust Agreement establish requirements for visitation and communication between the FOCI Company and the foreign parent/Affiliates. They include meetings at:

- Any location within or outside the U.S.
- Any facility owned or operated by the Company
- Any of the Affiliates or foreign parent at the discretion of the GSC

Any deviations from the Agreement must be approved prior to implementation by DSS. DSS requires advance approval of visits; however, defers to the GSC to determine the appropriate advance notice. Once the GSC has determined the suitable advance notice for the visit it must be formalized in writing to DSS. The Visitation Procedures by the designated Proxy Holders or Voting Trustees is the same process discussed in Module 3 in the Government Security Committee, except:

- The Proxy Agreement does not have routine visits and designates at least one (1) Proxy Holder to approve the visit(s).
- The Voting Trust Agreement does not have routine visits and designates at least two (2) Voting Trustees to approve visits.

DSS will defer to the GSC on what constitutes an unforeseen exigency visit, so long as visits are reviewed and approved after the event.

Refer to Course Resources link, Module 4.

### *4.6 Accepting Shares or Dividends*

What does it mean to a Proxy Holder or Voting Trustee to accept Shares or Dividends on behalf of a company? We will take a look at both starting with the Proxy Holder.

**Proxy Holder Shares or Dividends**

The Shareholder appoints the Proxy Holders as its proxies to have all the rights, powers, and authority to exercise all the voting rights with respect to the Shares. The Shareholders will annotate all certificates representing the Shares with the legend. All certificates representing the Shares should be deposited with the Proxy Holders at their office in trust for the Shareholder and available for review by DSS, and receipt for the certificates provided to the Shareholder. In the event the Proxy Holder receives any shares as a dividend, the Proxy Holder should accept such shares. The shareholder is entitled to receive payments equal to cash dividends, if any, for those Shares from the Proxy Holders.

**Voting Trustees Shares or Dividends**

The Shareholder has transferred and assigned to the Voting Trustees all of the Shares of the Corporation, and are registered in the name of the Voting Trustees. During the term of the Agreement, no shares of the Corporation should be held by the Shareholder, but all Shares should be deposited with the Voting Trustee. In the event the Voting Trustee receives any shares of capital stock of the Corporation held the Voting Trustee they should accept such Shares of the Corporation and issue Voting Trust Certificates. The Shareholder, or any successor Shareholder, is entitled from time to time to receive from the Voting Trustees payments equal to cash dividends, if any, for those Shares.

Refer to Course Resources, Module 4.

### *4.7 Proxy Holders Voting Discretion*

The Proxy Holders are entitled to exercise their sole and absolute discretion, with respect to any and all of the Shares at any time covered by the Proxy Agreement. Proxy Holders have the right to vote or consent to any and every act of the Corporation as if they were absolute owners of the Shares. All decisions and actions by the Proxy Holders should be based on their independent judgment and free of any control or influence from the Shareholder.

The Proxy Holders should consult with the Shareholder concerning these actions so the Shareholder may have sufficient information to ensure that all such actions will be taken in accordance with applicable United States laws and regulations.

Refer to the Course Resources link, Module 4.

### *4.8 Voting Trustees Voting Discretion*

The Voting Trustees must make decisions for the Company independent of the Shareholder or Shareholder(s) (collectively known as the Affiliated Group). When the Trustees meet for the purpose of voting the Shares, only the Trustees may vote and they cannot give that responsibility to any other board member. The Trustee must protect the legitimate economic interests of the Shareholder in the Corporation as an ongoing business concern.

The Trustees are entitled to exercise in their sole and absolute discretion, the right to vote the same or to consent to any and every act of the Corporation based on their independent judgment with respect to the Shares covered under the Voting Trust Agreement. The Shareholder has the right, however, to forward written suggestions for the Trustees consideration, except for suggestions on persons to be nominated as successor Voting Trustees. Each written notice from the Shareholder should be immediately provided to DSS for review.

The Trustees should consult with the Shareholder on these actions so that the Shareholder may have sufficient information to ensure that all such actions will be taken in accordance with applicable United States laws and regulations.

Refer to the Course Resources link, Module 4.

### *4.9 Proxy Holders and Voting Trustees Compensation*

The terms of compensation includes any and all benefits (including travel and other administrative expenses) that are negotiated between the Proxy Holders/Voting Trustees and the Shareholder. These benefits should be paid by the Company and remain in effect throughout their tenure of the Proxy Holders/Voting Trustees.

A copy of the compensation terms should be provided to DSS. This compensation should be paid promptly by the Company according to the provisions in the Agreement.

### *4.10 Annual Review and Certification*

The Voting Trust Agreement and Proxy Agreement are required to have an Annual Review/Annual Implementation and Compliance Report and Meeting as outlined in Module 6.

The Voting Trustees should also include in the report the signed Voting Trust Certificate which is approved by the Voting Trustees and subject to approval by DSS. In the event a Voting Trust Certificate becomes mutilated, destroyed, lost or stolen, the Voting Trustees may, in their sole discretion, issue and deliver a new Voting Trust Certificate representing a like number of the Shares of the cleared Corporation. There are two ways to reissue Certificate:

If the Certificate is mutilated, the voting Trust Certificate should be exchanged and canceled.

If the Certificate was destroyed, lost, or stolen, then the Voting Trust Certificates should be issued upon production of evidence of such destruction, loss or theft that is satisfactory to the Voting Trustees and upon receipt of indemnity satisfactory to them.

Refer to the Course Resources link, Module 4.

### *4.11 Module 4: Conclusion*

You have completed Module 4, on the Additional responsibilities of the Proxy Holders and Voting Trustees which covered the:

- Proxy Agreement vs Voting Trust Agreement
- Meetings with the shareholder(s)
- Visits and communications
- Accepting Shares or Dividends
- Voting Discretion
- Compensation of Proxy Holders/Voting Trustees
- Annual Review and Certification

## Module 5 (IS187.16) - Security Vulnerability Assessment and Best Practices at FOCI Companies

### *5.1 Module 5: Introduction*

Welcome to Module 5 on the Security Vulnerability Assessment. Under the National Industrial Security Program, (NISP), the DSS mission has oversight on the protection of U.S. and foreign classified information and technologies in the hands of industry. DSS is the DoD Cognizant Security Office for industrial security and responsible for managing and administering the NISP for DoD and other federal agencies to provide the Government Contracting Activities with assurances that contractors:

Are eligible for access to classified information and

Have systems in place to properly safeguard the classified information for which they have access.

Assuring that all security practices and procedures are established and maintained by contractors is completed through the Security Vulnerability Assessment (SVA) process.

### *5.2 Module 5: Objectives*

The objective for this module is to discuss how the SVA process is conducted.

- What the SVA covers for FOCI Companies
- Assessment of the FOCI Agreement implementation plans and security measures
- Government Security Committee's (GSC's), Facility Security Officer (FSO), Technology Control Officer (TCO), Senior Management Official (SMO) roles and responsibilities in preparation for the FOCI portion of the assessment
- Security assessment ratings
- Recognition for Superior Ratings and the James S. Cogswell Outstanding Industrial Security Achievement Awards
- Reasons for Poor Security Ratings and Undue Influence
- Enhancements and Best Practices
- Categories of vulnerabilities
- Reporting changed conditions on a FOCI company

### *5.3 SVA Overview*

So, what is an SVA? It is the periodic security review of all cleared contractor facilities by DSS to ensure that safeguards employed by contractors are adequate for the protection of classified information in compliance with the National Industrial Security Program Operating Manual (commonly known as the NISPOM) requirements.

SVAs are conducted as a collaborative effort between DSS and the cleared contractor's Key Management Personnel (KMPs) and employees for both U.S. and FOCI mitigated companies. The SVA for FOCI companies are conducted within 60 calendar days prior to the Annual Implementation and Compliance Meeting (see Module 6 for more information).

### *5.4 FSO Responsibility*

As a member of the GSC, it is important that you understand what DSS will require for the initial and subsequent SVAs.

The FSO will advise the GSC of the following:

- Establishment of a security program for the FOCI Company, including the HQ and any Cleared Subsidiaries or Branch/Division Offices
- Using the security requirements and methods of protecting classified contracts (DD Form 254)
- Based on the FOCI Agreement Implementation Plans
- If an SSA company, communicates the status of all National Interests Determination (NIDs) for access to proscribed information
- Maintenance of the Personnel Security program
- Security Education Program and Resources
- Establishing and evaluating the Company's security countermeasures.
- Obtaining threat information from DSS Counterintelligence
- Suspicious Contact reporting to DSS Counterintelligence
- Insider Threat program
- Policies and procedures for implementation and compliance to the FOCI Agreement and its implementation plans to include:
    - Technology Control Plan (TCP),
    - Electronic Communications Plan (ECP),
    - Affiliated Operations Plan (AOP),
    - Facilities Location Plan (FLP), and
    - Visitation Policy (could include Routine/Non-routine business visits and Social Contacts based on the FOCI Agreement)

Note: Refer to the company's FOCI Agreement and see Module 5.

### *5.5 TCO Responsibility*

The TCO advises the GSC on the implementation and process of the TCP:

- Establishing security measures
- Prevent inadvertent access by non-U.S. citizen employees and visitors to unauthorized information
- Assure access by non-U.S. citizens is limited to information for which Federal Government disclosure authorization is obtained (e.g. export license or technical assistance agreement)
- Unique badging, escorts, segregated work areas, security training, etc.

### *5.6 Security Assessment Ratings*

At the end of the SVA, DSS will review and identify the vulnerabilities. DSS assigns one of the following assessment ratings: Superior, Commendable, Satisfactory, Marginal, and Unsatisfactory.

**Superior** - reserved for contractors who have consistently and fully implemented the requirements of the NISPOM in an effective fashion resulting in a security posture of the highest caliber.

**Commendable** - is assigned to contractors who have fully implemented the requirements of the NISPOM in an effective fashion resulting in an exemplary security posture.

**Satisfactory** - is the most common rating and de that a contractor's security program is in general conformity with the basic requirements of the NISPOM.

**Marginal** - indicates a substandard security program. This rating signifies a serious finding in one or more security program areas.

**Unsatisfactory** - is the most serious security rating. It is assigned when circumstances and conditions indicate that the contractor has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified material in its possession or to which it had access.

For additional information refer to the Course Resources link, Module 5.

### *5.7 Cogswell Award*

The James S. Cogswell Award, established in 1966, is a coveted award in the industrial security community. The award criteria focus on principles of industrial security excellence. It is given for outstanding achievement in matters related exclusively to a contractor's security program.

The Cogswell Award selection process is rigorous. A DSS Industrial Security Representative (commonly known as an IS Rep) may only nominate facilities that have at a minimum <u>two consecutive Superior SVA ratings</u> and must show a sustained degree of excellence and innovation in their overall security program management, implementation, and oversight.

### *5.8 Poor Rating Reasons*

FOCI companies may receive a poor security rating due to undue influence from the foreign parent/Affiliates in the following areas:

- Unapproved affiliated services
- Influencing or involved in the hiring, firing, and performance appraisals of FOCI Company employees
- Using shared payroll services to withhold payment to FOCI Company employees
- Foreign parent/Affiliates attempting to shift delivery timelines on classified contracts

- Reporting structures that circumvent the FOCI Company's governing body (GSC)
- Unapproved collocation with foreign parent/Affiliates
- Network connections with foreign parent/Affiliates not identified in an approved ECP
- Unreported changed conditions to senior management, foreign ownership, investments, or acquisitions and mergers

### *5.9 Categories of Vulnerabilities*

The DSS Representative will provide the company FSO with a list of identified vulnerabilities, NISPOM references, and recommended actions to remedy. Vulnerabilities subtract from the overall assigned security rating.

Categories of vulnerabilities include:

**Acute Vulnerability** - Acute Vulnerability -classified information is at imminent risk of loss or compromise or has already resulted in loss or compromise. Immediate corrective action is required.

*Example*: Could be release of information on a classified contract to the foreign parent or transfer of classified information over unsecure network.

**Critical Vulnerability** - may place classified information at risk of loss or compromise.

*Example*: Could be unapproved affiliated services, collocation, or ECP.

**Administrative Vulnerability** - all instances of non-compliance with the NISPOM that are not acute or critical. Some of these vulnerabilities can be corrected on the spot.

*Example*: Could be the establishment of the GSC was not set forth in the corporation's bylaws, visitation approvals do not meet the specified timeline, or employees were not briefed on the purpose of the ECP and their responsibilities under the plan.

### *5.10 Enhancements*

An enhancement directly relates to and improves the protection of classified information beyond the baseline NISPOM standards. Enhancements add to the overall assigned security rating. In order for the company to receive credit for enhancements, the company must first meet the baseline NISPOM requirements in that area.

- Areas where a company can introduce enhancements include:
- Company sponsored events
- Internal educational brochures/products
- Security staff professionalization
- Information/Product sharing within the community
- Active membership in security community
- Contractor self-inspection
- Threat identification and management
- Threat mitigation
- FOCI/International

- Classified material controls/physical security
- Information systems

Refer to the Course Resources link, Module 5.

### *5.11 Best Practices*

A best practice is an enhanced process implemented to adequately manage a security program. Items that are considered to be FOCI best practices are:

- Strong GSC and management support that is fully engaged on the requirements of the FOCI Agreement and supportive of the security staff
- Completion of the Outside Director/Proxy Holder training
- Continuous communication with DSS to ensure transparency on matters pertaining to FOCI

### *5.12 Change Condition Reporting*

A "Changed Condition," according to NISPOM (Paragraph 1-302g), is a change to a contractor's organizational and/or financial structure, which could affect the contractor's facility clearance. According to the FOCI lifecycle in Module 1, the Changed Condition should be reported to DSS upon occurrence. These changes could include:

- Change of ownership or stock transfers that affect control of the company
- Change of the operating name or address of the company or any of its cleared locations
- Change in KMP
- Actions to terminate business or operations for any reason (e.g. reorganization, bankruptcy, or any change that might affect the FCL)
- Material change in FOCI which should be reported on the SF 328

The Industrial Security Letter (ISL) is issued periodically to inform Industry, User Agencies, and DoD Activities of developments relating to industrial security. The ISL is for information and clarification of existing policy requirements.

Refer to the Course Resources link, Module 5.

### *5.13 Module 5: Conclusion*

You have completed Module 5, we discussed what the SVA covers for FOCI Companies and how the FSO and TCO advise the GSC. We also discussed the security assessment ratings and enhancements/best practices, Cogswell Award, reasons for poor security ratings, categories of vulnerabilities, and reporting changed conditions.

### Module 6 (IS188.16) - Initial Meeting, Annual Compliance Report, and Annual Meeting

#### *6.1 Module 6: Introduction*

Welcome to Module 6, on the Initial and Annual Compliance Meeting. Once the FOCI Mitigation Agreement has been agreed upon by all parties, an Initial Meeting will take place between DSS and the Company. Thereafter, an Annual Implementation and Compliance Report is prepared by the Company and presented to DSS on the anniversary month of the Agreement. This is the Annual Implementation and Compliance Meeting.

This module will take you through what to expect during the Initial Meeting, the criteria for the Report, and the Annual Implementation and Compliance Meeting. In this Module, you will see how the agreement is set in place with the Initial Meeting, the criteria for the Annual Implementation and Compliance Report, and what takes place during the Annual Implementation and Compliance Meeting.

Let’s start with the objectives for this Module.

#### *6.2 Module 6: Objectives*

The objectives for Module 6 are:

- Define the purpose of the Initial Meeting
- Identify the key players
- Describe the two parts
- Illustrate how to prepare the Annual Implementation and Compliance Report
- Define the purpose of the Annual Implementation and Compliance Meeting
- Identify the key players
- Describe the two parts

#### *6.3 Signatory Location*

The Initial and Annual Implementation and Compliance Meeting will take place at the FOCI Signatory location. The FOCI Signatory location is the Headquarters of the Company and where the Government Security Committee (GSC) resides.

#### *6.4 Initial FOCI Agreement Meeting*

The purpose of the Initial Meeting is to address the Company’s basic obligations under the security agreement being implemented to mitigate the FOCI. All parties involved (the cleared Company, the foreign parent, and DSS) will discuss any remaining questions or concerns.

This meeting is conducted by the DSS FOCI Operations Division Action Officer in accordance with the meeting agenda template, and is held in two separate parts.

Now, let’s discuss the first and second part of the Initial Meeting and what key players are involved in each part.

### *6.5 1st Briefings*

During the Initial FOCI Meeting, the mitigation agreement is reviewed and it will be signed by the Company. The FOCI Signatory provides a minimum of three signed original copies of the mitigation agreement at the Initial Meeting.

The meeting is conducted in two parts. In the **first part** of the Initial Meeting, the DSS representatives meet with the Outside Directors, Proxy Holders, or Voting Trustees only. No other parties are allowed to participate; this includes the Company's Facility Security Officer (FSO). The parties cover the following areas:

- Explain the Outside Directors, Proxy Holders, or Voting Trustees roles and responsibilities under their agreement
- Answer any questions regarding the agreement
- Review pertinent sections of the agreement such as the establishment of the Government Security Committee, limitations on the foreign interest, Technology Control Plan (TCP), Electronic Communication Plan (ECP), Affiliated Operations Plan (AOP), and visitation requirements.
- Discuss the current active classified contracts and government customers
- Agreement implementation requirements and timelines, and
- General FOCI and industrial security questions.

### *6.6 2nd Briefings*

During the **second part** of the Initial Meeting, the key players are the DSS representatives, the Outside Directors, Proxy Holders, or Voting Trustees, the whole Board of Directors, Facility Management, FSO, Technology Control Officer (TCO), Inside Director (SCA and SSA only), and Foreign Shareholder (optional).

The purpose of the second meeting is to provide the entire board with an overview of the requirements of the FOCI Mitigation Agreement as well as provide a forum for answering program and implementation-related questions. The parties discuss the following:

- Explain their roles and responsibilities under the agreement
- Discuss the requirements of the mitigation agreement
- Discuss DSS roles and responsibilities, including
- Field Office
- FOCI Operations Division
- Counterintelligence (CI) Special Agents
- Answer questions concerning the agreement implementation and timeline
- Discuss the active classified contracts and any contracts that maybe in the bid process
- Advise the Company of the procedures and policies that need to be developed and implemented
- General FOCI and industrial security procedures and questions

### *6.7 Agreement Expiration*

The FOCI Action Officer will bring back the signed copies (three each) of the mitigation agreement to DSS HQs to coordinate signatures by the Director, Industrial Policy and Programs who signs on behalf of the U.S. Government. The agreement is effective as of the date DSS signs the mitigation agreement. All formal mitigation agreements will have an expiration date of five years.

It is the responsibility of the company and its parent to notify DSS no later than 90 days prior to the expiration date with a proposed revised, restated or alternative agreement.

### *6.8 Annual Implementation and Compliance Report*

Just as with the Initial Meeting, the Annual Implementation and Compliance Report and Meeting verifies the Company's continuous obligations to ensure the security measures are being implemented.

A DSS Representative will contact the FSO to schedule the Annual Implementation and Compliance Meeting and request the submission of the Annual Implementation and Compliance Report. FOCI Signatories submit a draft Annual Report at least 30 days before the Annual Implementation and Compliance Meeting, or 10 Months Post FOCI Mitigation Execution. The Annual Meeting certifies compliance with the FOCI Agreement (including all TCP, ECP, AOP, FLP, and visitation requirements). The FSO should submit this report through e-FCL, a DSS database for the submittal of Company documents.

Refer to the Course Resources link, Module 6.

### *6.9 Annual Meeting*

DSS requires an Annual Implementation and Compliance Meeting with FOCI Signatories to discuss its security posture and compliance with the FOCI Mitigation Agreement. This Meeting is held during the anniversary month of the Agreement and also occurs after the annual Security Vulnerability Assessment (SVA) is conducted by DSS (see Module 5 for more information on the SVA). In preparation for the Annual Meeting,

DSS requires the following from the Company:

- The signed Annual Implementation and Compliance Report
- The Annual Meeting should be conducted at the FOCI Signatory Company location
- The Annual Meeting also occurs in two separate briefings.
- The DSS representatives are:
    - Industrial Security Representative
    - Field Office Chief
    - FOCI Action Officer
    - Senior Action Officer (optional)
    - Information System Security Professional (optional)

- CI Special Agent (optional)
- Regional Operations Manager (optional)

### *6.10 Annual Meeting Part 1*

**Part 1** of the meeting is led by DSS representatives, who provide the Meeting Agenda and meet with **only** the Outside Directors, Proxy Holders, or Voting Trustees.

During this part, the parties typically will discuss:

- Security posture of the facility and results of the SVA
- Answer any questions regarding the agreement
- Operational security-related issues
- Responsibilities of the Outside Directors, Proxy Holders, or Voting Trustees
- Any general industrial security, FOCI, or CI issues
- Issues with the foreign parent/Affiliate management or control
- New contracts or discontinued contracts
- National Interest Determination issues (SSA only)

### *6.11 Annual Meeting Part 2*

**Part 2** of the Annual Meeting is between DSS and the following Company representatives:

- Board of Directors
- Members of the GSC to include either Outside Directors, Proxy Holders, or Voting Trustees
- Key Management Personnel (KMPs)
- FSO and TCO
- Inside Director (SCA and SSA only)
- Foreign Shareholder (optional)
- Corporation's Chief Executive Officer (optional)
- Corporation's Chief Financial Officer (optional)

During this meeting, the parties discuss:

- Compliance with all board resolutions, special controls, practices, and procedures established to mitigate FOCI
- The Company's security posture (including all cleared locations operating under the Agreement)
- Acts of compliance or noncompliance with the terms of the agreement
- Any general industrial security and/or other specific FOCI issues
- Any necessary guidance or assistance
- Provide the Outside Directors, Proxy Holders, or Voting Trustees with a forum for providing a briefing of the Annual Implementation and Compliance Report
- DSS will obtain the signed Annual Report from the GSC Chairman and all the required Certificates

- Discussion on current and future classified contracts, NIDs, and discontinued contracts

### *6.12 Module 6: Conclusion*

You've just completed Module 6, the Initial Meeting and the emplacing of the Agreement; the Annual Implementation and Compliance Report and the Annual Meeting. We discussed who should attend which part of the Initial and Annual Meetings and what is discussed at each part of the Meeting.

Congratulations on completing all six modules of the Outside Directors, Proxy Holders and Voting Trustees training. Included with this training is Module 6 Job Aid, Red Flag Case Studies. It includes a sampling of six cases for your review of different Red Flag issues, FOCI concerns, challenges, DSS actions, Mitigation plan and the results.