OD/PH Module 3: Roles and Responsibilities of the Government Security Committee Student Guide

Table of Contents:

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 Foreign Ownership, Control, or Influence (FOCI) company is required to establish a permanent committee of its Board of Directors and the Outside Directors, Proxy Holders, or Voting Trustees, known as the GSC.

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

The Defense Counterintelligence and Security Agency (DCSA) 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.

Objectives

The objectives for this module are:

- Explain 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:
  - The Technology Control Plan (TCP)
  - Electronic Communications Plan (ECP)
  - Affiliated Operations Plan (AOP)
  - Facilities Location Plan (FLP)
  - and the Visitation Policies
- Discuss the Quarterly Meetings;
- Describe how to prepare the Financial Reports to the foreign parent; and
- Discuss the Closed Sessions for classified, export-control, and/or controlled unclassified information.

Please note that throughout this module, the term "Affiliate" refers to both the foreign parent (foreign shareholder) and other companies owned by the foreign parent, including those located in the U.S.

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 regulations, 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). The typical structure includes a Chairman and Secretary as members; as well as the Facility Security Officer (FSO) and Technology Control Officer (TCO) as principal advisors to the GSC.

GSC Chairman

The Chairman of the GSC:

- Is an Outside Director, Proxy Holder, or Voting Trustee designated by the GSC who designates a Secretary of the GSC;
- Provides advice and consent in selecting and retaining the Facility Security Officer (FSO) and the Technology Control Officer (TCO); and
- Prepares the Annual Implementation and Compliance Report along with the Chief Executive Officer (CEO).

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; and
- Preparing and retaining other documents sent to or received by the GSC and made available for inspection by DCSA.

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.

It is not permitted for the company to remove the FSO without the advice and consent of the Chairman of the GSC.

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.

It is not permitted for the company to remove the TCO without the advice and consent of the Chairman of the GSC.

GSC Performance Standards 1

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, and the Affiliates.

GSC Performance Standards 2

They should also advise DCSA 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.

GSC Performance Standards 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.

GSC Performance Standards 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.

GSC Performance Standards 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.

GSC Performance Standards 6

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

GSC Performance Standards 7

Each member of the GSC must execute and submit to DCSA, 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;
2. The U.S. Government has placed its reliance on him or her as a U.S. citizen and as a 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 agrees to be bound by and accepts his/her responsibilities under the Agreement.

GSC Performance Standards 8

The GSC must oversee that 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 Affiliates. This includes the directors, officers, and employees.

GSC Performance Standards 9

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, Proxy Holders, or Voting Trustees 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 DCSA.

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

Compliance Program & Policies

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

- Technology Control Plan (TCP),
- Electronic Communications Plan (ECP),
- Affiliated Operations Plan (AOP), and
- Facilities Location Plan (FLP).

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

Technology Control Plan

The purpose of the Technology Control Plan (TCP) is to preclude the possibility of inadvertent access by non-U.S. citizens or foreign nationals assigned to or employed by cleared companies to classified or export-controlled information for which they are not authorized.

The TCP describes all security measures in place to prevent such access and should address both the:

- Physical access (such as buildings, restricted areas, etc.) and
- Technical access (such as 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).

Refer to Course Resources link, Module 3 for more information.

Electronic Communication Plan

The purpose of the Electronic Communications Plan (ECP) is to maintain policies and procedures enabling effective oversight of communication between company personnel and the Affiliates to prevent their exertion, influence, or control over the company's business.

The GSC must ensure the company takes the necessary action, and maintains oversight to provide assurance to itself and DCSA 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 and could also include data storage, or the Cloud;
- Video conferences, cell phones, and facsimile;
- Internet, instant or text messaging, and email;
- Collaboration applications; and
- Network connectivity and infrastructure.

The ECP must:

- Include a detailed network configuration diagram that clearly shows all communications networks and facilities used by the company for the transmission or storage of electronic communications;
- Delineate which networks will be shared and which should be protected from access; and
- Describe network firewalls, physical and logical access controls, remote administration, monitoring, maintenance, retention, and the electrical and physical separation of systems and servers, as appropriate.

Refer to Course Recourses link, Module 3 for more information.

Affiliated Operations Plan

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

Typically these services are routine operations and do not relate directly to classified or export-controlled work. Companies operating under a FOCI Mitigation Agreement must receive prior approval from the GSC and DCSA before using any shared services.

Some examples of shared services are:

- Receiving administrative or other services from an Affiliate;
- Providing such services to an Affiliate;

- Sharing an employee/person between the FOCI company and an Affiliate;
- Sharing a third-party service provider with an Affiliate;
- Using Affiliate technology products; or
- Having commercial arrangements in the form of contracts and subcontracts, joint research, development, marketing or other types of teaming arrangements with an Affiliate.

The shared services to be provided must not violate the FOCI Mitigation Agreement and should be included in the AOP. DCSA approves the services in the AOP before the company can engage in using the shared services.

The GSC will:

- Submit the AOP for DCSA approval, ensuring no unapproved operations are occurring at the FOCI company.
- Notify DCSA of any proposed changes to an AOP and receive DCSA approval in writing prior to them occurring.
- Certify annually that the AOP is effectively executed and that the shared services do not circumvent the requirements of the FOCI Mitigation Agreement.

AOP Risks

Affiliated Operations Risk Factors:

- Allow an Affiliate to exert undue control or influence over the FOCI company or employees;
- Permit access by an Affiliate to employee adverse information;
- Permit access by an Affiliate to customer accounts and data;
- Prevent company from demonstrating ability to comply with all requirements of the FOCI Agreement.

Facilities Location Plan

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

The company must have written approval from DCSA of an FLP prior to collocating. The company and the GSC must demonstrate to DCSA 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;
- 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 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.

The GSC is responsible for:

- Overseeing the development and implementation of the FLP;
- Submitting the FLP for DCSA 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 DCSA 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.

DCSA identification of an unreported FOCI Collocation may negatively impact the status of the FOCI company's Facility Security Clearance.

Refer to Course Recourses link, Module 3 for more information.

Visitation Plan

The purpose of the Visitation Plan is to ensure visits with the Affiliates are controlled as required by the FOCI Mitigation Agreement.

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

Visit Requests are required for:

- All personnel who represent any of the Affiliates, including all the directors, officers, employees, representatives, and agents.
- Meetings at any location within or outside of the U.S. to any facility owned or operated by Affiliates.
- Video conferences and teleconferences (at the discretion of the GSC).

As an exception, the Inside Director, if attending company board meetings or company Board Committee meetings, does not need a Visit Request.

Approval of Visit Requests.

All requests for visits must be submitted or communicated in advance through the FSO to the designated Outside Director, Proxy Holder, or Voting Trustee 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

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:

- Purpose of the visit;
- Appropriate documents (such as designated forms), and
- Date and time of the visit.

The GSC, in its reasonable business discretion, may 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, Proxy Holder, or Voting Trustee.

Some examples of 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 review of commercial performance, products, suppliers, or solicitations.

Routine Business Visits do not involve:

- Key Management Personnel (KMP);
- The transfer or receipt of classified information;
- Export-controlled information; or
- Activities bearing upon the company's performance of its classified contracts.

The Outside Director, Proxy Holder, or Voting Trustee, along with the FSO, should also maintain a record of all Visit Requests.

This record should:

- Include all approved or disapproved requests;
- Provide information regarding completed visits (such as the date, place, personnel involved, and summary of material discussions or communications); and
- Be periodically reviewed by the GSC and DCSA.

Refer to Course Recourses link, Module 3 for more information.

Quality GSC Meetings

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

At the discretion of the GSC, representatives of the foreign parent and the company's management personnel may also be invited to attend 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. This includes a chronological file of all Visit Requests, reports of visits, and contact reports. These records shall be maintained for review by DCSA.

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 financial 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 on the format for financial reporting. Proxy Agreements require DCSA approval of the financial report format.

Closed Sessions

Closed Sessions are any discussions of classified information and/or export-controlled information attended solely 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.

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,
- Quarterly GSC Meetings,
- Financial Reports, and
- Closed sessions.