OD/PH Module 5: Security Reviews and Best Practices at FOCI Companies Student Guide

Table of Contents:

Module 5 Introduction

Welcome to Module 5 on the security review and best practices at Foreign Ownership, Control, or Influence (FOCI) companies. Under the National Industrial Security Program (NISP), the Defense Counterintelligence and Security Agency (DCSA) mission has oversight on the protection of U.S. and foreign classified information and technologies in the hands of industry. DCSA is the Department of Defense (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.

Validating that all security practices and procedures are established and maintained by contractors is completed through the security review process.

Objectives

The objectives for this module include discussing:

- How the security review process is conducted and what it covers for FOCI companies;
- How the Facility Security Officer (FSO) and the Technology Control Officer (TCO) advise the Government Security Committee (GSC) regarding the security review;
- The security review rating;
- Reasons for a poor security rating;
- Best practices; and
- Reporting changed conditions at a FOCI company.

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.

Security Review Overview

So, what is a security review? It is the periodic review of all cleared contractor facilities by DCSA 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.

Security reviews are conducted as a collaborative effort between DCSA, the cleared contractor's Key Management Personnel (KMPs), and employees for both U.S. and FOCI-mitigated companies. The security review for FOCI companies is typically conducted within 60 calendar days prior to the Annual Meeting (see Module 6 for more information on the Annual Meeting).

FSO Responsibility

As a member of the GSC, it is important that you understand what DCSA will require for the initial

and subsequent security reviews.

The FSO will advise the GSC of the following:

- Establishment of a security program for the FOCI company, including the headquarters and any cleared subsidiaries or branch/division offices, that uses the security requirements and methods of protecting classified contracts (DD Form 254), based on the FOCI Agreement;
- If a Special Security Agreement (SSA) company, communicates the status of all National Interest Determinations (NIDs) for access to proscribed information;
- Maintenance of the Personnel Security program;
- Security education program and resources;
- Establishing and evaluating the company security countermeasures:
    - Obtaining threat information from DCSA Counterintelligence,
    - Suspicious contact reporting to DCSA 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 (which could include Routine/Non-routine Business Visits and Social Contacts based on the FOCI Agreement).

TCO Responsibility

The TCO advises the GSC on the implementation and process of the TCP.
Establishing security measures such as unique badging, escorts, segregated work areas, and security training:

- Prevents inadvertent access by non-U.S. citizen employees and visitors to unauthorized information; and
- Assures access by non-U.S. citizens is limited to information for which Federal Government disclosure authorization is obtained (for example: export license or technical assistance agreement)

Security Review Rating

At the end of the security review, DCSA will summarize the results, identify the vulnerabilities and issues, highlight areas in which the company is performing well, and recommend any improvements. In addition, DCSA will assign a security rating based on the company's security posture and FOCI mitigation effectiveness. The DCSA representative will provide the company FSO with a report of these factors, including recommended actions to remedy any vulnerabilities and issues.

Refer to Course Resources link, Module 5 for more information.

Reasons for a Poor Security Rating

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

- Unapproved affiliated services;
- Influencing or being involved in the hiring, firing, and performance appraisals of FOCI company employees;
- Using shared payroll services to withhold payment to FOCI company employees;
- Affiliates attempting to shift delivery timelines on classified contracts;
- Reporting structures that circumvent the FOCI company's governing body (GSC);
- Unapproved collocation with Affiliates;
- Network connections with Affiliates not identified in an approved ECP; and
- Unreported changed conditions to senior management, foreign ownership, investments, or acquisitions and mergers.

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, and
- Continuous communication with DCSA to ensure transparency on matters pertaining to FOCI.

Change Condition Reporting

A "Changed Condition" 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 DCSA 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 Facility Security Clearance (FCL)); or
- 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.

Module 5 Conclusion

You have completed Module 5. We discussed:

- What the security review covers for FOCI companies,

- How the FSO and TCO advise the GSC,
- The security review rating,
- Reasons for a poor security rating,
- Best practices, and
- Reporting changed conditions.