

Outside Director and Proxy Holder Training:
Module 2: Managing Foreign Ownership, Control, or
Influence (FOCI) Mitigation

Defense Security Service

February 2014





Training Objectives

- FOCI Control Procedures
 - FOCI Visitation
 - Electronic Communications Plan
 - Technology Control Plan
 - Affiliated Operations Plan
 - Facilities Location Plan
- Preparing for a FOCI Assessment
- Reviewing Relationships with the Affiliates
- Subsidiary Compliance
- FOCI Training
- FOCI Records
- National Interest Determinations





FOCI Control Procedures

- All FOCI Mitigation Agreements require the establishment of the following control documents*:
 - Visitation Procedures;
 - Electronic Communications Plan (ECP);
 - Technology Control Plan (TCP);
 - Other Implementation Procedures
 - Affiliated Operations Plan (AOP); and
 - Facilities Location Plan (FLP) for review of potential FOCI Collocation
- The Government Security Committee is responsible for reviewing and approving these documents by submitting a written certification to the DSS FOCI Operations Division via the cleared company's or in-process company's Electronic Facility Clearance (e-FCL) or FOCIHQ@dss.mil

* These control procedures are required for all FOCI Companies even if not explicitly addressed in the mitigation agreement





FOCI Control Procedures – Visitation Procedures

- All visits with the Affiliates must be approved in advance within the timeframe designated by the Government Security Committee
- FOCI Mitigation Agreements often differentiate between Visits and Routine Business Visits
 - Visits – Require advanced approval by the designated Outside Director or Proxy Holder
 - Routine Business Visits – Require advanced approval by the Facility Security Officer, and generally do not apply to Proxy Agreements unless approved by DSS
 - Visits that pertain only to the commercial aspects of the Company's business:
 - made in connection with the regular day-to-day business operations of the Company;
 - do not involve Key Management Personnel or senior officials of the Affiliates;
 - do not involve the transfer or receipt of classified information or Export Controlled Information; and
 - do not pertain to activities bearing upon the Company's performance of its classified contracts





FOCI Control Procedures – Visitation Procedures

- The Government Security Committee should periodically review visit requests to ensure sufficient information is provided and that visits are being approved by the correct individual
- Generally, visits that exceed 30 consecutive business days or cumulatively exceed 200 days in a single year require advance DSS approval
- Categorizing visits along the lines of DSS approved Affiliated Operations, the nature of the interactions, or other means to develop metrics can provide the Government Security Committee with significant insights into the areas of the Company's business with the greatest risk for violations to the FOCI Mitigation Agreement





FOCI Control Procedures – Electronic Communications Plan

- Demonstrates how the FOCI Company will monitor/control electronic communications (i.e. email, fax, phone) – including the company's unclassified network(s) - to ensure there is no unauthorized disclosure of classified or export controlled material.
- Ensures the FOCI Company's unclassified network(s) is separated from the Affiliates unless approved otherwise by DSS
- The Government Security Committee has the right to determine if video teleconferences and teleconferences should be categorized as visits (requiring advanced approval) or subject to reporting/logs after the fact





FOCI Control Procedures – Technology Control Plan

- Shall prescribe all security measures determined necessary to reasonably foreclose the possibility of unauthorized access to classified or export controlled information by non-U.S. citizen employees or visitors
- The TCP shall also establish measures to assure that access by non-U.S. citizens is strictly limited to only the information for which appropriate Federal Government disclosure authorization has been obtained.





FOCI Control Procedures – Affiliated Operations Plan

- Business functions or teaming arrangement with Affiliates of a FOCI mitigated company are not authorized. When a company desires to engage in such arrangements with any Affiliate the services must be approved by the GSC and DSS in advance or as set forth in your FOCI Mitigation Agreement. Relationships with the Affiliates requiring advance approval include:
 - Affiliated Services;
 - Shared Third-Party Services (a service that will be provided by a third party service provider to both the Company or any of its Controlled Entities and any of the Affiliates)*;
 - Shared Person; and
 - Cooperative Commercial Arrangement*
- The above require approval through an Affiliated Operations Plan prior to the FOCI Company engaging in the relationship
- The intent of the Affiliated Operations Plan is to provide DSS and the Government Security Committee 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

***may be approved in advance by the GSC with notification to DSS**





FOCI Control Procedures – Affiliated Operations Plan

- An Affiliated Operations Plan must address:
 - Description of the service, to include:
 - which entity will provide the service;
 - which entity is paying for the service;
 - how the shared service benefits the entities;
 - specific sub-categories of services;
 - procedures associated with providing the service;
 - technology to be utilized, including shared software, information systems and applications;
 - whether the technology described above is classified or export-controlled; types of information to be exchanged through the service;
 - whether any Key Management Personnel will be involved in the shared administrative service; and
 - include any supporting documentation such as examples, screenshots, network configuration diagrams or sample reports as attachments
 - Identification of risks associated with the proposed Affiliated Operation with proposed Mitigation Procedures; and
 - Compliance review procedures and documentation.





FOCI Control Procedures – Affiliated Operations Plan

- The Government Security Committee is responsible for:
 - Overseeing the development and implementation of the Affiliated Operations Plan
 - Submitting the Affiliated Operations Plan for DSS approval
 - Ensuring no unapproved Affiliated Operations are occurring at the FOCI Company
 - Ensuring that the FOCI Company notifies DSS of any proposed changes to an Affiliated Operations Plan prior to them occurring
 - Certifying annually that the AOP is effectively executed and that the Affiliated Operations do not circumvent the requirements of the FOCI Mitigation Agreement
- Any substantive change made to an existing Affiliated Operations Plan requires approval by DSS prior to the changes being implemented
- The nature and extent of a Company's FOCI plays a significant role in the DSS determination on the approval of an Affiliated Operations Plan





FOCI Control Procedures – Facilities Location Plan

- FOCI Collocation is when a FOCI Company is located within the proximity of an Affiliate, which would reasonably inhibit the company's ability to comply with the FOCI agreement.
 - Such scenarios may include location in the same building or campus.
 - Collocation is not authorized unless approved in advance by DSS.
- When a FOCI Company is located within close proximity of an Affiliate, DSS requires a Facilities Location Plan
- A DSS approved Facilities Location Plan establishes that FOCI Collocation is not present so long as all requirements of the FOCI Mitigation Agreement and Facilities Location Plan are met
- DSS identification of an unreported FOCI Collocation may negatively impact the status of the FOCI Company's Facility Security Clearance





FOCI Control Procedures – Facilities Location Plan

- The Facilities Location Plan is the vehicle for the FOCI Company and the Government Security Committee to demonstrate to DSS that being closely located to an Affiliate does not degrade the Company's ability to comply with its FOCI Mitigation Agreement
- The Facilities Location Plan must:
 - Identify organizational relationship between collocated entities (parent, affiliate, etc.)
 - 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





FOCI Control Procedures – Facilities Location Plan

- The Government Security Committee is responsible for:
 - Overseeing the development and implementation of the Facilities Location Plan
 - Submitting the Facilities Location Plan for DSS approval prior to the FOCI Company becoming located within close proximity to an Affiliate
 - Ensuring no FOCI Collocation is present at any of the FOCI Company's facilities
 - Monitoring the Facilities Location Plan to ensure all FOCI Mitigation requirements are met
 - Ensuring the FOCI Company notifies DSS of any proposed changes to a Facilities Location Plan 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
- The nature and extent of a Company's FOCI are important factors in the DSS determination on the approval of a Facilities Location Plan





Preparing for a FOCI Assessment

- The FOCI Company should:
 - Confirm all FOCI Control Procedures have been approved by the Government Security Committee and DSS, if required
 - Compare the extent of the relationships with the Affiliates to determine they are within the scope of, and managed consistently with, the DSS approved FOCI Control Procedures
 - FOCI Mitigation is unique and tailored for each individual company either through the language in the Mitigation Agreement and/or the FOCI Control Procedures
 - Maintain a record of all DSS approvals and denials
 - Proxy Companies are subject to an annual independent financial audit, and must provide DSS with confirmation that an audit has been completed
 - Identify any pending requests with DSS





Preparing for a FOCI Assessment

- Assess the implementation of FOCI Control Procedures to ensure:
 - Protection from Unauthorized Access of Classified Information
 - Protection from Unauthorized Access of Controlled Unclassified Information (CUI), i.e. Export Controlled information (ITAR & EAR)
 - Compliance with the DSS approved FOCI Control Procedures (Visitation, TCP, ECP, and, if applicable, AOP and FLP)
 - Undue Influence: Any action taken to control or influence the FOCI Company's classified contracts, its participation in classified programs, or its corporate policies concerning the security of classified information and export controlled information.
 - Operational Security (OPSEC)* - if any

* Additional security requirements required by the Government Contracting Activity typically established in the DD Form 254 (Contract Security Classification Specification)





Reviewing Relationships with the Affiliates

- Level of interaction with the Foreign Parent and/or Affiliates will vary significantly
- Use the FOCI Control Procedures to understand the nature of each relationship with the Affiliates, i.e.
 - Foreign Investment only
 - Marketing Arm of their Foreign Parent or U.S. Parent
 - Access Elsewhere/Services Firm
 - Integrating Affiliate components into U.S. equipment
- Assess whether the scope and frequency of interactions are consistent with approved Affiliated Operations and other FOCI Mitigation requirements
- Ensure Affiliate Operations and interactions are being managed consistently with the DSS approved plans





FOCI Subsidiary Compliance

- The FOCI Action Plan applies to the entire FOCI Company – including its subsidiaries and controlled entities as defined in the FOCI Mitigation Agreement - not just the cleared employees and cleared facilities
- Ensure FOCI Control Procedures are fully implemented across the entire corporation
- The FOCI Company should ensure that all employees understand their responsibilities under the FOCI Mitigation Agreement





FOCI Training

- FOCI training should ensure employees demonstrate a strong understanding of the following:
 - The intent of FOCI Mitigation;
 - Nature of the FOCI at the Company;
 - Requirements levied on employees per the FOCI Control Procedures:
 - Visitation;
 - Technology Control Plan;
 - ECP; and
 - If applicable, AOP and FLP
- Thorough FOCI Training is a strong indicator of strong FOCI Compliance Program





FOCI Records

- Ensure the following are maintained for review by DSS and the Government Security Committee:
 - Visit Logs;
 - Contact Reports;
 - Social Contact Reports;
 - Phone/Fax Logs;
 - GCA approval for use of Affiliate Technology;
 - Board Meeting Minutes; and
 - GSC Meeting Minutes
- Identify anomalies in interactions
 - Inconsistent with normal business
 - Did not obtain proper approval
 - High frequency of unnecessary interactions





FOCI Records

- Records provide the following insights:
 - Feel for their business
 - Relationship with the FOCI Company's Parent(s) & Affiliates
 - Does the FOCI Company Board run the company?
 - How much weight do the Inside Directors carry?
 - Feel for compliance/amount of energy/effort
 - Identify business areas and individuals which may require greater attention from the Government Security Committee





National Interest Determinations

- FOCI Companies operating under Special Security Agreements require a National Interest Determination (NID) prior to being granted proscribed information
 - Proscribed Information includes:
 - Top Secret
 - Communications Security (COMSEC), excluding controlled cryptographic items when unkeyed or utilized with unclassified keys
 - Sensitive Compartmentalized Information (SCI)
 - Restricted Data (RD)
 - Special Access Program (SAP)
- To facilitate the NID process the Government Security Committee should maintain a record of all classified contracts requiring access to proscribed information and the status of the NID
- The FOCI Company shall promptly notify DSS when a contract requiring a NID is awarded via NID@dss.mil
- The FOCI Company should educate each Government Contracting Activity of the NID requirement prior to the award of a contract can help expedite the process
- Verify with the Government Contracting Activity that access to proscribed information is actually required





References

- *FOCI Information*
- http://www.dss.mil/isp/foci/foci_info.html
- *FOCI Mitigation Instruments*
- http://www.dss.mil/isp/foci/foci_mitigation.html
- *FOCI Process In-process Companies*
- <http://www.dss.mil/isp/foci/in-process.html>
- *FOCI Process Acquisitions*
- <http://www.dss.mil/isp/foci/foreign-acquisitions.html>
- *FOCI Implementation Documents*
- <http://www.dss.mil/isp/foci/implementation-procedures.html>
- *NID Process*
- http://www.dss.mil/isp/foci/nat_interest_deter.html
- *Regulations*
- http://www.dss.mil/isp/fac_clear/download_nispom.html

