FOCI OPERATIONS DIVISION

RED FLAG CASE STUDIES

Reference: e-ISOM 16.6.6 Security Rating Calculation Worksheet

FOCI OPERATIONS DIVISION DEFENSE SECURITY SERVICE

For Internal Use Only

CASE STUDY

Company A, Proxy Agreement

FOCI OPERATIONS DIVISION

RED FLAG ISSUE

During an annual SVA, the IS Rep identified that the foreign national President of an affiliate company was hired to be the full-time VP of Finance for Company A. The foreign national is resident at the Company A cleared facility and maintains both positions. An approved visit request is in place for 365 days to allow the individual to provide senior management services to the affilate, which is a holding company.

FOCI CONCERN

Shared Employee

- Not properly identified by Company A as an affiliated service for GSC and DSS approval
- Unclear to DSS how visitation and communication with this individual is monitored
- Visit request approved by Company A for excessive duration
- Although VP, Finance is not an Officer position, it appears high level to employees
- Has ability to take any actions on behalf of the affiliate company
- Foreign national resident in cleared facility – does the TCP address this?
- DSS entrusted the Company A GSC with approval authority for shared employees; why did the GSC approve the visit request without questioning the shared employee relationship?
- Why wasn't the shared employee relationship disclosed to DSS immediately upon consummation to allow opportunity for questions, per Company A FOCI requirements?
- Company A's seven Proxy Holders did not appear to be fully aware of the scope of this shared employee relationship

CHALLENGES

- High visibility KMP and GSC
- Company A's history of Superior compliance

DSS ACTIONS

1. IS Rep and FOD AO notified respective chains of command of red flag following SVA
2. IS Rep gathered substantiating documents from Company A to establish timeline of events
3. IS Rep requested corrective action plan from Company A with 15 day suspense
4. IO and IP internally discussed red flag and security rating
5. IO and IP met with Company A security team to brief red flag and security rating
6. IO and IP internally planned exit briefing with support from IO and IP Directors
7. IP Director separately addressed DSS concerns with the GSC Chairman
8. IO led successful exit briefing with Company A security team and Senior Management Official

MITIGATING PLAN

IS Rep received an adequate corrective action plan from Company A

- Proposed AOP revision addressing shared employees in greater detail
- Additional rigor in Company A shared employee approval process (two-person integrity, enhanced GSC review)
- Escalation of shared employee requests to corporate security team
- Increased coordination between corporate security and group security leads regarding affiliated operations
- Audit of all active visit requests for excessive duration
- Potential early termination of existing shared employee arrangement

RESULT

Ratings matrix indicated a Superior rating
DSS issued a critical vulnerability and withheld two enhancements, resulting in Commendable rating
With red flag, DSS lowered rating to Satisfactory

CASE STUDY

Company B, Special Security Agreement

FOCI OPERATIONS DIVISION

RED FLAG ISSUE

During the annual SVA, the FOD AO identified that Company B shares unapproved finance affiliated operations with an affiliate company. Company B and its affiliate company are collocated with DSS approval. The FOD AO discovered that Company B issued badge access to four affiliate company employees, and the affiliate gave badge access to some of Company B's employees. Some of these employees are KMP; for example, the affiliate's senior management official was granted badge access to the Company B command suite.

FOCI CONCERN

Affiliated Operations

- Operating in accordance with previously disapproved finance services
- Company B's request for an integrated Finance Department was disapproved by DSS in May 2013 because it required Company B personnel to report to affiliate company
- Shared finance services may allow inappropriate glimpse into company financials related to classified contracts
- Shared finance services may allow undue influence over budget and headcount

Collocation

- Granting badge accesses into each company's space precludes effectiveness of the approved FLP
- Company B approved recurring 30 day visit requests with insufficient, very broad justification to support this access. DSS could not ascertain the purpose or details of the approved visits.
- Collocation reduces ability to comply with SSA visitation procedures; this demonstrates the importance of closely monitoring collocation arrangements

CHALLENGES

- High visibility KMP and GSC
- Approved collocation lent itself to increased amount of visitation

DSS ACTIONS

1. IS Rep and FOD AO notified respective chains of command of red flag following SVA
2. IS Rep and FOD AO immediately mandated termination of finance services and revocation of badge accesses
3. IO and IP internally discussed red flag and security rating
4. IO and IP internally planned exit briefing with support from FOD Chief
5. IO led successful exit briefing with Company B security team
6. Company B submitted a written request to DSS for a long-term visit for the interlocking CFO of Company B and the affiliate to provide financial reporting, forecasting, tax and treasury services to both companies under the direction of Company B
7. DSS reviewed and approved the request
8. FOD AO coordinated a letter to Company B notifying the company of DSS concerns pertaining to their relationship with the affiliate company

MITIGATING PLAN

DSS received an adequate corrective action plan from Company B

- Restructured request into a reverse affiliated operation
- Addressed performance evaluations and other HR matters for shared CFO
- Identified expected frequency, nature, and purpose of interactions in detail
- Immediate revocation of badge accesses

RESULT

Ratings matrix indicated a Commendable rating

With red flag, DSS issued a critical vulnerability, resulting in a Satisfactory rating

CASE STUDY

Companies C & D, Special Security Agreements

FOCI OPERATIONS DIVISION

RED FLAG ISSUE

Upon ECP compliance issues being escalated to FOD, FOD identified significant concerns with the structure and management of these two sister SSA companies. FOD identified that Company C was effectively managed by a foreign national. Further communication with the companies revealed that management was inappropriately vested to executive committees, on which interlocking directors served. Both companies shared interlocking officers with their affiliates, creating collocation issues. Company C operated pursuant to a disapproved AOP. The companies had unacceptable and unapproved ECPs and did not properly implement their SSA visitation policies.

FOCI CONCERN

SSA

- Control over companies was not properly vested to the SSA Board of Directors, which significantly weakens the structure of the SSA
- Non-U.S. citizen serving as senior management official, likely able to make decisions on behalf of the cleared company and bind the cleared company contractually
- Two interlocking officers identified at Company D – how are their interactions being monitored? Who pays them?

ECP

- Unapproved, despite SSAs being in place since 2007
- Cleared companies subject to global IT network services brokered by the foreign parent
- Unclear if foreign parents have admin rights or access to cleared companies' servers

Affiliated Operations

- Operating pursuant to disapproved shared services
- Other affiliated operations not properly identified for DSS approval
- DSS has no assurances of FOCI risk mitigation measures associated with services

Visitation

- Company D Inside Director resident at cleared facility and involved in day-to-day operations
- Scope of visitation policy fell short of SSA requirements – it was not applied consistently to all cleared company employees

CHALLENGES

- Historical precedence –Company C and Company D operated this way since 2007
- Non-compliance is deeply rooted in the organizational structure of the Companies C and D
- Bringing the companies into compliance required significant restructuring and costs

DSS ACTIONS

1. At the SVA, the IS Rep issued a critical vulnerability for unapproved affiliated operations.
2. FOD later issued additional vulnerabilities concerning management controls, a resident Inside Director, and interlocking officers and directors.
3. FOD coordinated extensively with IO Field, Region and HQ elements regarding FOCI concerns.
4. DSS invalidated FCLs of Company C, Company D, and their cleared subsidiaries.
5. Company C and Company D submitted an FCL revalidation plans to DSS.
6. IO and IP coordinated to conduct compliance SVAs at each company.
7. DSS revalidated FCLs of Company C, Company D, and their cleared subsidiaries.

MITIGATING PLAN

DSS received adequate corrective action plans from both Company C and Company D

- Company C submitted an FCL action plan to include an internal reorganization, elimination of interlocking directors, an AOP, an ECP, an FLP, and a revised visitation policy
- Company D submitted a Commitment Letter addressing management structure issues, an FLP, an AOP, an ECP with milestones, and compliance SVA by DSS. The FCL revalidation plan included the submission of progress updates to DSS.

RESULT

DSS issued critical vulnerabilities at Company C and Company D
With red flag, the SVAs resulted in Unsatisfactory ratings
DSS invalidated FCLs; following revalidation, the companies have Satisfactory ratings

CASE STUDY

Company E, SSA

FOCI OPERATIONS DIVISION

RED FLAG ISSUE

DSS experienced ongoing difficulties in requiring Company E to memorialize all affiliated operations in an AOP. Company E disclosed to DSS sharing of extensive IT services, to include help desks, global IT services contracts, and multiple shared third-party providers. As a self- described matrix organization, Company E decentralizes business functions internationally. Consequently, Company E and its affiliates exchange some level of affiliated operations within almost all traditional business and overhead functions. At the SVA, DSS identified systemic non-compliance with the SSA due to the absence of an approved AOP.

FOCI CONCERN

Affiliated Operations

- Operating pursuant to unrequested affiliated operations
- Company was unable to advise DSS of the quantity, nature and extent of all affiliated operations
- With shared employees, DSS could not ascertain how visitation and communication are monitored
- DSS had no assurances related to FOCI risk mitigation within implemented services
- Reporting chains and management were unclear to DSS

CHALLENGES

- High visibility KMP and GSC
- Pure volume of affiliated operations across all business functions required Company E to start from the ground up
- Lack of existing documentation at Company E related to affiliated operations

DSS ACTIONS

1. IS Rep and FOD AO notified respective chains of command of red flag following SVA
2. IO and IP internally discussed red flag and security rating
3. IO and IP internally planned exit briefing with support from IO and IP Directors
4. IO led successful exit briefing with Company E security team
5. IO and IP, with support from the FOD Chief, met with Company E to communication expectations with a suspense date
6. FOD AO met with Company E security team to understand scope of AOP
7. FOD AO coordinated with Company E on an ongoing basis to establish an acceptable AOP format and review drafts until a mutually agreeable plan was finalized
8. DSS continuously engaged with the Company E GSC at the next quarterly Board meeting to ensure GSC involvement and oversight of the AOP

MITIGATING PLAN

Company E worked with DSS to provide an appropriate AOP for DSS review and approval within the suspense date

RESULT

Ratings matrix indicated a Commendable rating
With red flag, DSS issued a critical vulnerability and lowered the rating to Satisfactory

CASE STUDY

Company F, Proxy Agreement

FOCI OPERATIONS DIVISION

RED FLAG ISSUE

Company F operates under a PA due to ownership by a parent company, which is majority owned a dual citizen of Australia and Canada and CEO of an affiliate company. Historically, Company F and the affiliate company were collocated under an approved FLP. The affiliate consolidated staff under Company F and maintained the affiliate as a holding company with no employees. As a result, the FLP was no longer needed and Company F adopted a new name. In July 2013, DSS conducted an SVA at Company F and awarded a Superior rating. In Fall 2013, the Company F CEO reported a potential cyber intrusion to DSS in which an unknown actor obtained unauthorized access to unclassified proprietary documents. In January 2014, the Company F FSO submitted a memo to the GSC and DSS regarding possible violations of the PA and stating his resignation. The allegations were related to unapproved visits, collocation concerns, and IT technology merge resulting from the consolidation of Company F and its affiliate. Around the same time, DSS received media inquiries from various reporters about a potential Company F security violation involving classified information.

FOCI CONCERN

Visitation, PA principles

- If undocumented visits occur, the FSO, GSC, and DSS cannot accurately understand the relationship between Company F and its affiliates or be assured that there are no unauthorized transfers of export-controlled or classified information. Further, we cannot determine if the affiliates are exercising an unacceptable level of influence over the company's business operations
- Potential unauthorized access to classified information by foreign CEO
- Apparent lack of GSC involvement or oversight
- Potential perception to government customers that Company F and its affiliate are not distinct business entities

CHALLENGES

- Management of unsupported whistleblower allegations and media inquiries
- High visibility KMP

DSS ACTIONS

1. DSS asked the GSC to provide a written response to the FSO's memorandum and submit any necessary changes to the FOCI implementation plans, as needed
2. DSS IO and IP coordinated to consolidate comments on the GSC's response to the allegations; IO notified OAG of allegations
3. DSS met with the Proxy Holders to review the GSC's response and discuss the FSO's departure. The GSC believed the issues to be anomalies somewhat related to personality conflicts between the Company F and CEO. DSS asked the GSC to exercise more diligent oversight and discussed whether existing security procedures needed changing.
4. DSS IO and IP determined that a follow-up, out of cycle SVA was needed with FOD involvement. DSS determined that the FOCI-related vulnerabilities were not deliberate and were inadvertently related to the recent organizational changes
5. DSS met with Company F to discuss the issues raised by the media and follow up on the reported cyber intrusion. DSS determined the media allegations were unfounded
6. DSS leadership in IP and IO managed media inquiries by coordinating with Public Affairs office. DSS HQ shared transcripts with Field, Region, and Company F

MITIGATING PLAN

Company F GSC worked with DSS to resolve issues related to the perception of Company F and its affiliate as one company, the appointment of a replacement FSO, and potential ECP concerns. DSS conducted a follow-up SVA and provided ongoing advice and assistance.

RESULT

With red flag issue, DSS conducted an accelerated, follow-up SVA to determine validity of FOCI-related vulnerabilities, and concluded that the company has a Satisfactory security posture. DSS committed to schedule ongoing assistance visits over the next 6 months to validate compliance.