NAVIGATING THE AFFILIATED OPERATIONS PLAN:

A GUIDE FOR INDUSTRY

Business Analysis and Mitigation Strategy Division, DSS

CONTENTS

AOP LIFE CYCLE

Reviewing affiliated operations that may pose a FOCI risk is a continuous process, from identifying shared services to DSS approval and oversight.

The **AOP Life Cycle** diagram illustrates your company's role in each step of this continuous process.

SURVEY internal administrative and operational functions to identify Affiliated Operations

Identify **RISKS** presented by each Affiliated Operation

Work with relevant **EMPLOYEES** to develop risk mitigation measures

DESCRIBE Affiliated Operations, risks, mitigation measures and corresponding oversight, for DSS approval

Ensure **COMPLIANCE** with the processes outlined in the approved AOP

INTRODUCTION

The purpose of this guide is to assist companies with mitigating and managing affiliated operations per the requirements of the Foreign Ownership, Control, or Influence (FOCI) mitigation agreement.

The guide may not include all potential areas of affiliated operations, but it offers a starting point for Facility Security Officers (FSOs) and Government Security Committees (GSCs) in developing an AOP. We will discuss three important topics:

1. How to identify whether your company has any affiliated operations, and if so, which;
2. How to write an AOP for DSS's review and approval; and
3. How to manage your affiliated operations for internal and external assessments.

First, however, we pause to consider the purpose of AOPs and affiliated operations more generally.

Competition, best business practices, and responsibility to stockholders have driven industry to identify areas where processes can be streamlined to increase efficiency.

DSS used to refer to affiliated operations as "shared services" because affiliated operations often involve a mitigated company sharing a service with its affiliates. DSS's understanding of what form that sharing can take, however, has evolved, and no longer just includes services that an affiliate provides to the mitigated company.

DSS considers an affiliated operation to be a business or operational relationship between a mitigated company and an affiliate, to include any internal policy, process, or procedure that could give an affiliate financial or operational leverage over the mitigated company.

This definition covers "reverse shared services," where a mitigated company provides a service for an affiliate, because those "reverse services" can still leave the mitigated company vulnerable to FOCI or the inadvertent dissemination of classified or otherwise sensitive information.

Affiliated operations can help companies save time and money, but they can also introduce new risks, presenting subtle and complex mitigation challenges.

DSS introduced the AOP as a way to identify affiliated operations so that industry can maintain competitiveness while reassuring DSS that FOCI is mitigated.

Ultimately, the goal of the AOP is to reconcile DSS's mission with industry's needs. As those needs evolve, so too may the AOP.

IDENTIFYING AFFILIATED OPERATIONS

Whether your company is in process for a facility clearance (FCL) or long established in the National Industrial Security Program (NISP), it probably shares some services with or through an affiliate that must be reviewed by your GSC and approved by DSS.

Identifying those services can be a challenge, especially if you are not used to thinking of shared services as "affiliated operations."

DSS encourages you to use this guide as a resource for analyzing your company's affiliated operations, and to foster a productive dialogue with your FOCI action officer.

TYPES OF AFFILIATED OPERATIONS

This section will introduce several categories of commonly shared services with questions designed to help you to understand which services you share, how you can describe them, what FOCI risks they present, and how you can mitigate and continuously monitor those risks.

FOCI mitigation agreements define affiliated operations as cooperative endeavors, regardless of whether such endeavors, performed directly or through third party service providers, are administrative, operational or commercial.

These endeavors include shared personnel, shared third-party services, commercial arrangements, other shared services and products, and affiliate technology. Most affiliated operations have to be approved by DSS before the mitigated company can begin using them.

There are several considerations that can help you with the process of analyzing your

company and identifying which operations, if any, involve your affiliate(s).

FIRST, *Does sharing the service give my company an economic benefit it would not otherwise enjoy?*

For example, suppose an affiliate uses software for payroll processing and offers to provide it to your company for a below-market fee.

If you accept the affiliate's offer, it will save your company money, but the affiliate will also acquire a degree of leverage over your company; in a worst-case scenario, the affiliate could threaten to cancel the software sharing arrangement. This may compel you to purchase the software from a third party at higher cost, potentially harming your company's financial wellbeing.

Because sharing the software therefore gives the affiliate leverage over your company, that sharing counts as an affiliated operation and must be described in your AOP. If the affiliate provides services rather than goods, the test for economic benefit is still satisfied.

SECOND, *Does using an internal process or procedure of either the affiliate or my company give the affiliate some operational leverage over my company?*

For example, suppose an affiliate asks your company to provide annual reports on your employees' compensation, ostensibly to standardize salaries throughout the corporate family. Providing that information may be helpful in fostering corporate symmetry and competitive pay, but it also gives the affiliate insight into how you manage part of your company's business; such insight could enable activities which may constitute undue leverage over your company. As such, this counts as an affiliated operation that must be included in your AOP.

THIRD, *Does my company provide a benefit to the affiliate that it would otherwise not enjoy?*

This consideration involves a "reverse shared service," where a mitigated company provides a service to an affiliate, rather than the other way around.

Here the mitigated company may acquire leverage over the affiliate, but risks of inadvertent disclosures of information and undue influence can still arise, and still have to be mitigated.

For example, suppose an affiliate asks you to provide accounting services to them. Doing so would result in your providing a service to the affiliate it would not otherwise enjoy, making this arrangement an affiliated operation that must be described in your AOP.

FOURTH, *Is my company using the same third party vendor or service provider my affiliates use?*

For example, suppose a mitigated company wishes to use an insurance company to

provide medical benefits to its employees, and it happens that the affiliate uses the same insurer for its own employees. Because both the mitigated company and the affiliate are using the same third party entity, this is an affiliated operation that must be described in your AOP.

FIFTH, *Is my company engaged in a contract, joint research and development or teaming agreement with the affiliate that is commercial and arms-length in nature?*

For example, suppose your company wishes to subcontract performance on part of a commercial contract involving the distribution of widgets.

You could conceivably engage any number of companies to assist with such distribution, but you decide to engage an affiliate since the work is unclassified and you have greater familiarity with their operations and reliability.

Since you enter into this commercial agreement with the affiliate independently and on (more or less) equal footing, you are engaging in a cooperative commercial arrangement, which must be described in your AOP.

SIXTH, *Does my company share personnel with an affiliate?*

For example, suppose an affiliate asks you to allow one of your accountants to serve as its Treasurer on a part-time basis. Permitting the accountant to do so would constitute sharing an employee, making this arrangement an affiliated operation.

CATEGORIES OF AFFILIATED OPERATIONS

In this section we will discuss the different categories of affiliated operations to assist you in defining the specifics of your circumstances. The examples below are notional and therefore may not apply perfectly to your company.

An AOP should be comprehensive, describing all operations and services the mitigated company shares. It should also be detailed enough to explain all risks

that are inherent to that sharing, and how the company will mitigate those risks and conduct oversight.

The AOP should empower the GSC to take an active role in overseeing the company's affiliated operations, but it should also explain how DSS can conduct its own oversight. The AOP, in short, is both a security plan and a governance plan, and DSS emphasizes both in its review.

Also, please note that the suggested mitigation measures discussed below are neither perfectly inclusive nor exclusive, and DSS may require additional steps on a case-by-case basis.

Human Resources

The scope of potential Human Resources (H.R.) services is expansive, covering everything from assistance in hiring to termination of benefits.

Some examples of H.R.-affiliated operations are as follows: leveraging your affiliates' subject matter expertise in conducting job interviews; advertising job openings on an affiliate's website; sharing consolidated reports on compensation.

Sharing H.R. services can present FOCI risks because of the leverage that might be acquired by your affiliates, although some of those risks can be mitigated with robust GSC oversight.

When reviewing H.R. services, DSS is interested in how much information affiliates can learn about your company's employees, including the projects they work on. DSS is also interested in the affiliates' ability to affect the pool of prospective employees if it assists in the hiring process.

Furthermore, DSS is interested in the amount of leverage the affiliates have over hiring, firing, compensation and performance appraisal decisions. Some questions you should consider include:

- *How does my company perform recruitment functions — advertise vacancies, receive resumes, interview applicants, select a candidate (especially cleared personnel and Key Management Personnel [KMPs])?*
- *If vacancies are advertised on an affiliate's website, does the affiliate "screen" resumes before they are sent to my company?*
- *How does my company handle performance evaluations for employees, including company officers? Who is responsible for determining compensation, particularly for cleared personnel and KMPs?*
- *Are my company's employees able to participate in affiliate training programs, including employee exchange or mentorship opportunities?*
- *How are my company's H.R. processes audited, and by whom?*
- *How is payroll managed? Do my company and the affiliate share a system?*

The risks involved in H.R. services include exposure of details related to operations security (OPSEC) established by the Government Contracting Activity (GCA) pursuant to contract requirements; identification of classified programs and employees; and undermining the managerial independence of the mitigated company (to include influence over salaries and compensation).

These risks may be mitigated by carefully reviewing all information that is shared with the affiliates to ensure that the identity of individuals with personnel security clearances and details about their projects are not included, and by ensuring that all personnel decision-making authority rests with the mitigated company. The amount of mitigation required will depend on the amount of influence the affiliates might be able to exert when personnel decisions are made.

Finance and Accounting

Your affiliates are entitled to receive information about your company's financial situation on a regular basis. But a company might wish to share more than information with its affiliates; perhaps you want to share a bank account for cash flow purposes, or perhaps your affiliate wants to file consolidated tax returns for your company. The ultimate parent may wish to standardize accounting procedures throughout the corporate family.

Given the importance of accounting in corporate governance, leveraging financial services must be considered and monitored carefully. (Audits are discussed separately.)

When reviewing requests for affiliated operations in the financial arena, DSS will look to ensure that the GSC is able to review the procedures used to report information to the affiliates. If the affiliates wish to assist with accounting services, the mitigated company must maintain control and oversight of its own books.

As with H.R. services, the mitigated company must consider how the requested services might allow the affiliates to obtain leverage, thereby unduly influencing its decision making. The mitigated company must also consider whether the services might compromise its financial viability. Some questions you may want to consider include:

- *How does my company report financial data to its affiliate(s), and does the GSC review the data or the format of the reporting in advance?*
- *When my company reports financial data, is a shared network connection used?*
- *How does my company manage budget development, and who has final approval authority?*
- *How does my company manage accounts payable/receivable?*
- *Does my company share a cash pool or bank account with the affiliate, and does the affiliate have either deposit or withdrawal authority?*

- *How are taxes done for my company, and does the GSC review the format of reporting tax information to the affiliates?*

The risks associated with finance and accounting services include exposure of OPSEC details; undermining the managerial independence of the mitigated company; adversely affecting short-term cash flow; and unduly influencing long-term project financing and budget decisions.

These risks can be mitigated by: having the GSC review and approve the format for reporting all financial data; aggregating and screening data respecting classified programs; masking locations, employees, and customer line items; reserving the right to obtain financial services from a third party; ensuring that the mitigated company's board maintains the ability to pay for operations expenses without affiliate intervention; and ensuring that the Board retains final decision-making authority.

Internal Audits

As part of accounting operations, some affiliates may want to play a role in conducting regular audits of your company.

While this can be helpful in promoting uniform practices throughout a corporate family and identifying irregularities, it can also potentially enable the affiliates to learn about a mitigated company's classified projects and cleared employees; it can also unduly influence the company's operational independence.

For those reasons, you may find the threshold required for being allowed to conduct an internal audit is typically higher than other shared services.

If the affiliates request internal auditing as a service, DSS is interested in the safeguards emplaced to prevent the inadvertent disclosure of classified and other sensitive information. DSS will also consider how the results of the audit are conveyed to the mitigated company, and whether the GSC is empowered to accept or reject any suggestions corresponding to those results. Some questions you should ask include:

- *How are internal audits of my company's processes and/or finances conducted and by whom precisely? Will the audits be conducted by internal auditors or third-party auditors?*
- *Who determines the scope, schedule, and methodology of the internal audits, and is the GSC empowered to approve it all?*
- *How will my company prevent the auditors from obtaining even inadvertent access to sensitive information?*
- *Who receives the results and findings of the internal audits, and is the GSC empowered to review those findings before they are sent to the affiliates? How are they then protected?*
- *Who has decision-making authority over the adoption of auditor recommendations?*

Some of the risks of conducting internal audits have been discussed above, but others include the inadvertent disclosure of OPSEC and other sensitive information; compromising the managerial independence of the mitigated company; inviting undue influence on process improvements that might affect performance on classified contracts; relying on an affiliate for a business-critical function; and identifying employees and their work.

Possible mitigation strategies include the mitigated company maintaining an internal audit capability or using a third party auditor; heavily involving the GSC in the development of the internal audit scope and process (affiliate expertise may be used while developing the scope of the audit, however the audit must be conducted by internal or third-party auditors); empowering the security staff and GSC to monitor the audit and review all information, including the audit's results, before being shared with the affiliates; allowing the mitigated company's board to have sole authority to accept or reject internal audit recommendations.

Business Development

Leveraging business development (BD) operations with affiliates could take the form of contracting support, sales, research and development (R&D), or supply chain coordination.

This coordination could allow the affiliates to assume an oversized role in the managerial decisions of the mitigated company, presenting clear and important FOCI risks that must be mitigated.

When DSS reviews affiliated BD operations, it will be especially concerned with ensuring that all decision-making authority rests with the mitigated company's board. DSS will scrutinize carefully any arrangement that empowers the affiliates to act or speak on behalf of the mitigated company.

DSS will also consider the extent to which procurement activities affect the supply chain for a product being used by the U.S. Government, and how that supply chain is secured. If the mitigated company wishes to sub-contract work to an affiliate, or be a sub-contractor for an affiliate, DSS will examine how the GSC monitors and oversees the arrangement, and how the government customer is notified. Some questions you may ask include:

- *How does my company identify prospective BD opportunities and clients, and how do the affiliates assist with those processes, if at all?*
- *Do the foreign affiliates liaise directly with government customers on behalf of my company, or have any representational authority?*
- *Does my company resell or license products or services of the foreign affiliates in connection with procurement activities?*
- *Does my company use foreign affiliate technology in the performance of classified or unclassified contracts?*

- *What involvement if any do affiliates have in my company's R&D?*
- *If my company enters into a sub-contract agreement with an affiliate, how will the GSC monitor the project to ensure there is no undue FOCI?*

The potential risks of leveraged BD services include exposure of OPSEC and other sensitive information; undermining the managerial independence of the mitigated company; supply chain vulnerabilities; and confusion among government customers about which corporate entity is providing a service or product.

These risks can be mitigated by ensuring the affiliates are not authorized to represent or bind the mitigated company in contract; testing affiliates' technology/products prior to delivery to the government customer; reserving all ultimate BD decisions, including choice of vendors, to the mitigated company; notifying the government customer anytime the cleared company uses technology, products or services from an affiliate in the performance of classified contracts (a copy of such notification must be included as an addendum to the AOP); and making all affiliated commercial arrangements arms-length transactions.

Marketing

While advertising and other affiliated marketing operations are relatively straightforward, DSS will consider whether affiliate involvement compromises the mitigated company's operational independence. Some questions you may ask include:

- *How does my company manage marketing, particularly trade shows, press releases, branding, and client services?*
- *Does my company provide contract or program information to the affiliates for marketing purposes?*
- *Do the FSO and the Technology Control Officer (TCO) review marketing information before it is sent to affiliates, and do they report to the GSC on the matter?*
- *How much independence does my company have in its marketing plans and strategies?*
- *Can my company obtain the same marketing services from a third party?*
- *Is my company required to participate in any marketing-related activities at the affiliates' behest?*

The potential risks of sharing marketing services include exposure of OPSEC details and other sensitive information, and compromising the mitigated company's operational independence.

Most marketing-related risks can be mitigated by requiring the FSO to review any information prior to release to the affiliates; notifying the GSC if any problems arise; distinguishing the mitigated company from the affiliates within marketing materials; and reserving ultimate decision-making authority to the mitigated company.

Legal

If your company uses an affiliate's general counsel when appearing before a government agency, obtaining guidance on how to comply with legal requirements, or having an affiliate review regulatory submissions for compliance and quality control purposes, then you are sharing legal services.

Even if your company is not looking to "share" a lawyer as such, asking for even non-binding legal advice constitutes an affiliated operation that must be mitigated.

Given the weight legal counsel can carry at all levels of a company, DSS will scrutinize shared legal services carefully to ensure that the affiliates' counsel do not act as unregulated agents of the mitigated company.

DSS will also be sensitive to potential conflicts of interest that may arise, especially with respect to mitigating undue FOCI. Some questions you should ask include:

- *How does my company receive legal counsel, and is counsel required to execute any non-disclosure agreements?*
- *Does my company have its own general counsel?*
- *Can my company afford to hire outside counsel if necessary?*
- *Do the affiliates have legal regulatory obligations that depend upon compliance by my company?*
- *Is the affiliates' counsel empowered to represent my company in litigation, contract negotiations, or other transactions with third parties?*
- *How will the affiliates' legal counsel conduct conflict screenings, and what will (s)he do if a conflict is identified or even suspected?*
- *Who is compensating the attorney, and for which services?*

The potential risks of using affiliated legal operations include inadvertent leakage of sensitive information to affiliate personnel; undermining the mitigated company's managerial independence; relying on an affiliate for a business-critical function; and conflicts of interest.

Potential mitigation strategies can include requiring the GSC to approve all legal consultations in advance; hiring a general counsel at the mitigated company;

reserving the right to seek outside counsel at the GSC's discretion; barring the affiliates from representing the mitigated company in any negotiation or before any tribunal; and empowering the mitigated company to accept or reject any advice offered.

Shared Personnel

While sharing personnel presents unique opportunities, it also presents unique risks that must be considered carefully.

Shared personnel include *(i)* affiliate employees assigned to work with the company or *(ii)* company employees assigned to work with any affiliate.

Shared personnel are not permitted absent DSS approval. Sharing personnel can create conflicts of interest and greatly affect the work of a mitigated company, depending on the employees' position.

For example, sharing project engineers can heighten the risk of leakage, while sharing accountants or attorneys can have an undue impact on the mitigated company's management. The mitigated company may have to implement a facility location plan (FLP), subject to review and approval by DSS, to accommodate a shared employee. Additional visit control measures might be necessary.

Sharing personnel, in other words, can require a considerable amount of work by both the affiliates and the mitigated company to accommodate the arrangement.

Should you request to share personnel, DSS will analyze the role intended for the shared individual(s) to determine how much influence (s)he is likely to have on the mitigated company's management and operations.

DSS will also work with the company to devise appropriate collocation mitigation measures via a FLP. This analysis will be the same whether an affiliate shares personnel with a mitigated company, or vice versa. Some questions you should ask include:

- *Are any individuals employed by both my company and its affiliate(s), and if so, what sort of work do they do?*
- *If my company hosts affiliate employees, how often do they interact with the affiliates, and what is the nature of those interactions?*
- *If my company hosts affiliate employees, how are their communications with the affiliate monitored?*
- *If my company hosts affiliate employees, are they authorized to supervise or otherwise direct any of the mitigated company's employees?*
- *Do the affiliates host any of my company's workers as long-term visitors, and if so, what is the nature of those visits?*
- *If the affiliates host any of my company's employees, what steps are taken to ensure they are not unduly influenced by the affiliates?*

The potential risks of sharing personnel include inadvertent disclosure of sensitive information to affiliate personnel; undermining the mitigated company's managerial independence; undue influence on employees performing on classified contracts; and conflicts of interest.

While an FLP may go some way toward mitigating some of these risks, other **potential mitigation measures** include avoiding the identification of classified programs and cleared personnel; ensuring that the mitigated company retains all personnel-related decisions for its own employees (e.g. hiring, firing, etc.); having the shared employee become an employee of the mitigated company; requiring all hosted affiliate personnel to take training on the FOCI mitigation agreement and all related, ancillary plans; and creating an oversight structure to report non-compliance by shared personnel, as well as inappropriate attempts to influence cleared individuals.

AOP SUBMISSION

DSS provides a formatted template of AOPs for FOCI companies' use in preparing drafts. The template standardizes submissions from all FOCI companies.

It defines broad categories of shared services to include affiliated services (traditional and reverse), shared third party services, shared persons, and cooperative commercial arrangements.

The AOP ensures that all FOCI risks have been addressed and provides guidance for review of risk mitigation strategies. For each service or operation shared between the mitigated company and foreign affiliates, the mitigated company is expected to provide a description of the service, the risks inherent in sharing the service, corresponding risk mitigation measures, and review of the service internally by the company and externally by DSS.

This can be done by working with relevant employees and executives to identify and develop risk mitigation measures. Lastly, the AOP must be approved by DSS before the mitigated company can start leveraging any affiliated operations.

This section will introduce the DSS template AOP and provide guidance on how to prepare and submit a draft AOP for DSS review and approval.

- **STEP 1:** Download the AOP template, which can be found on the DSS website: **www.dss.mil/isp/foci/affiliated-operations-plan.html**

- **STEP 2:** On the template title page *(page 1)*, replace "Defense Security Service FOCI Operations Division" with your company's name. The word "Template" under "DSS Affiliate Operations Plan" should also be removed. "February 2013" should be replaced with AOP submission date.

- **STEP 3:** On page 2, add the full date of submission, Company name, address, CAGE code, and the names of all affiliates with which you will share services.
- **STEP 4:** On the table of contents *(page 3)*, replace the "X's" with actual page numbers once the draft AOP is finalized. The instructions located at the bottom of page 3 can remain or be removed.
- **STEP 5:** On the "WHEREAS" clause page *(page 4)*, fill in "[COMPANY]" and "[PARENTS/AFFILIATES]" in the title and first paragraphs with your corresponding Company name and Parent/Affiliate names. The second WHEREAS clause should reflect the date of your Company's executed FOCI mitigation agreement. The remainder of the "WHEREAS" clauses should not be changed; any proposed alterations must be approved by DSS.
- **STEP 6:** "ARTICLE I. PLAN OF AFFILIATED OPERATIONS" *(starting on page 4 and ending on page 6)* should not be changed, and any proposed alterations must be approved by DSS.
- **STEP 7:** "ARTICLE II. AFFILIATED PRODUCTS AND SERVICES" *(starting on page 6 and ending on page 7)* should not be changed, and any proposed alterations must be approved by DSS.
- **STEP 8:** For "ARTICLE III. AFFILIATED OPERATIONS" *(page 8)*, replace "[SERVICE TYPE]" (under "1. AFFILIATED SERVICES, A.") with the title of the affiliated operation being requested.

Under subsection i., "Service Description," describe in detail the service you want to share. The Service Description for each and every affiliated operation requested should include the following information:

- Who will provide the affiliated operation to whom and why? Who will pay for it, and what is the benefit of sharing it? What would it cost for the company to do it themselves?
- How will the recipient and the provider implement the affiliated operation?
- Does the mitigated company have access to other options, or is leveraging the affiliated operation mandatory?
- What technology will be utilized, and is any of it owned by the affiliate? Is the technology classified or export-controlled? What types of information will be exchanged, and is it either classified or export-controlled?
- Will KMPs be involved, and if so, how? What will be the frequency of interaction between the mitigated company and affiliates, and how will such interaction take place?

- Supporting documentation such as examples, screenshots, network configuration diagrams or sample reports should be included as attachments within the Schedule of

Supporting Documents section at the end of the AOP.

- **STEP 9:** The following must be included in section ii., "Risk/FOCI Mitigation Procedures" for each and every affiliated operation requested:
    - Describe the specific risks associated with sharing the operations and identify the mitigation procedures that will be used to mitigate those risks.
        - Risks inherent in sharing affiliated operations could include: lack of independence from affiliates (including financial or economic leverage); inadvertent disclosure of classified, sensitive and/or OPSEC information; undue influence on cleared employees performing on classified contracts; and conflicts of interest.
        - Risk Mitigation Procedures are tools and processes to prevent undue influence and/or unauthorized disclosure of sensitive information.
- **STEP 10:** The following must be included in section iii. "Review of Service" for each and every affiliated operation requested:
    - What specific steps will the GSC take internally to ensure compliance? How will the FSO and TCO participate in those steps?
        - Describe how the GSC has properly considered potential risks associated with the approval of the affiliated operations and what their plan is to emplace controls to mitigate those risks.
    - What documents can DSS review and which employees can it interview to ensure compliance?
- Except as otherwise provided in the Mitigation Agreement, for classified contracts where a mitigated company will use affiliate technology, products or services, the mitigated company's management shall notify each applicable Government Contracting Activity (GCA) about the affiliate technology, products or services (unless the GCA has waived its right to notification in writing). The GCA's approval shall be maintained by the mitigated company for the duration of the applicable classified contract and must be made available for review upon request.
- **STEP 11:** Pages 9 and 10 provide examples of how to execute Steps 8-10 above. Page 9 uses a risk matrix to outline the Risk/FOCI Mitigation Procedures and Review of Service, while page 10 uses the traditional approach. Either method will suffice for submission.
- **STEP 12:** Repeat Steps 8-10 for "2. SHARED THIRD-PARTY SERVICES" *(page 11)*.
- **STEP 13:** Repeat Steps 8-10 for "3. SHARED PERSONS" *(page 12)*.
- **STEP 14:** Repeat Steps 8-10 for "4. COOPERATIVE COMMERCIAL ARRANGEMENTS" *(page 13)*.

- **STEP 15:** For "ARTICLE IV. ACKNOWLEDGEMENTS" *(page 14)*, provide signed statements from both the mitigated company and the affiliates who will be party to the affiliated operations, acknowledging that if serious and/or systemic acts of non-compliance with the FOCI mitigation agreement are identified DSS may require immediate termination of the shared service.
- **STEP 16:** "Exhibit A DEFINITIONS" *(pages 15-17)* should not be changed, and any proposed alterations must be approved by DSS.
- **STEP 17:** In "SCHEDULE OF SUPPORTING DOCUMENTS" *(page 18)*, the Company must include copies of any necessary exhibits (such as: joint venture agreements, purchase orders, invoices, third-party engagement letters, screenshots, network configuration diagrams and sample reports) relevant to the requested affiliated operations, for review by the GSC and DSS.
- **STEP 18:** "ATTACHMENT 2" *(page 19)* may be used for any additional documentation that may be required.

DSS is responsible for approving all affiliated operations. DSS may determine that some operations are either inconsistent with the intent of the FOCI mitigation agreement or else present unacceptable risk that cannot be sufficiently mitigated, and therefore will not approve them.

The AOP template should be used for initial draft submissions. Companies can submit the draft AOP to their DSS FOCI Action Officer (AO) directly or through their local Industrial Security Representative (ISR).

The AO and mitigated company will negotiate the language of the AOP, which usually entails two or three redline drafts.

Once the final draft is submitted by the mitigated company, the AO will coordinate with the corresponding DSS Field Office, Regional Office, Office of General Counsel and senior leadership to obtain final approval or disapproval. DSS may require GCA concurrence prior to approving shared services.

The mitigated company may receive additional feedback during the internal coordination process since multiple DSS offices can voice concerns at any point during their review.

AOP reviews are very thorough because the AOP is often the most detailed governance document a mitigated company uses. Furthermore, DSS's goal is to have a high level of assurance that the procedures in the AOP can effectively mitigate FOCI risks. Collaboration with DSS while identifying and defining services is critical to minimize review time.

- Common themes and misconceptions:
    - *"This service presents no FOCI risks":* Sharing a service always presents FOCI risk because any sharing allows the parent/affiliates to have a certain degree of leverage over

the mitigated company, which may affect the company's independence over its operations of the classified program(s) or information.

- *"This service presents no FOCI risks because we have already mitigated them":*
  Risks must be identified and defined, notwithstanding any existing mitigation measures.

- *"Classified information is not at risk because ours is a non-possessing facility":*
  There are many ways classified or otherwise-sensitive information can be compromised.

- *"The Review of Service section applies only to DSS review, not the GSC":*
  The Review of Service section is intended to show how both DSS and the GSC will conduct oversight of each service.

DSS will not approve affiliated operations when the corresponding FOCI risks cannot be sufficiently mitigated. Some examples include:

- The individuals performing the service(s)/operations may have unauthorized access to classified or sensitive information in the performance of their duties.
- The mitigated company cannot demonstrate ability to comply with the mitigation agreement.
- The mitigated company does not appear to be a separate entity from its affiliates to DSS, its employees, or its government customers.
- The AOP results in a determination by DSS that a company mitigated with a Proxy Agreement or Voting Trust is not financially viable or sufficiently independent.
- The affiliated operations would allow an affiliate to exert undue control or influence over the mitigated company or its individual employees.
- The affiliated operations would permit access by an affiliate to government customer accounts and data.

AOP COMPLIANCE

A mitigated company may not permit an affiliated operation to circumvent the requirements of the AOP or the mitigation agreement. The mitigated company must therefore only use affiliated operations that have been approved by DSS.

If, however, an affiliated operation is leveraged prior to DSS approval due to unusual circumstances, the mitigated company must promptly notify DSS of the situation.

Nothing in the AOP constitutes a waiver of any requirement in the mitigation agreement or the NISPOM, including controls on communications and visits.

If unapproved affiliated operations are identified, whether or not there is an existing AOP, they may affect the status of the facility security clearance (FCL). Unapproved affiliated operations identified during a DSS Security Vulnerability Assessment (SVA), may have a significant impact on the final security rating. This section will outline compliance with the AOP.

In anticipation of DSS's review, ensure that the mitigated company is in compliance with the processes outlined in the approved AOP.

Furthermore, in connection with its annual reporting obligations under the mitigation agreement, the GSC must certify that it is effectively monitoring the affiliated operations, and that those operations do not allow the affiliates to exercise undue control or influence over the mitigated company; allow unauthorized access to sensitive government information; or introduce new and unmitigated risk.

During the SVA, DSS will assess whether or not an AOP has been approved. Any and

all approved affiliated operations will be reviewed to ensure compliance with the AOP. Documentation must be provided as evidence of compliance. If third party service providers have been approved, the separate contracts/engagement letters may be reviewed. Employees with knowledge of the approved affiliated operations should be available for interview.

- Questions that a mitigated company can ask itself before an SVA:
    - Does my company use affiliate employees in a long-term visitor arrangement to support affiliated operations?
    - If my company maintains staff to support affiliated operations, to whom do those individuals report?
    - Has the security staff/GSC identified any instances of non-compliance with the AOP since the last vulnerability assessment?
    - Were appropriate corrective actions taken in response to acts of AOP non-compliance? Were all issues and their resolution reported to DSS?
    - Who holds the contract/engagement letter for shared third-party providers?
- The following questions are meant to address specific functional areas of your company:
    - **IT:** Do any of the affiliated operations require an IT connection from my company to the affiliate (e.g. shared financial data system or H.R. system)? If connected, are firewalls and encryption sufficient to mitigate unapproved access? Is sensitive information stored on the network? Can my company's employees access the foreign entity's IT system or an intranet/extranet, or vice versa? If entities have access to a shared intranet/extranet, do the mitigated entities have the ability to upload or download materials? If so, under what conditions? Who has access approval authority? What individuals have administrative rights and whom do they work for? Do the companies use a SharePoint-like site for information sharing? Who monitors information that is shared, uploaded or downloaded? Do the companies use videoconferencing services and/or equipment, or else the same phone, internet, and cable provider? If so, do they have separate contracts with the provider(s)? Who provides help desk services for employee IT troubleshooting? Who provides maintenance for my company's systems, and are the providers in-house or external? Who has access to the IT access control lists (ACLs)? Where are the IT hub and servers, and their backups, physically located? Are any of the IT support personnel non-US citizens? Do the IT system design, defenses, and procedures protect

export controlled information from unauthorized disclosure? **Have all of the affiliated operations been reflected in the Electronic Communications Plan (ECP)?**

- **Financial Systems/Services:** For Proxy Agreements or Voting Trust Agreements, has the financial information format been approved by DSS and GSC? What is the process when an affiliate has questions about the data transmitted? Does the GSC review the data before it is forwarded? Is any classified contract, customer, or program identifying information sent to an affiliate? Does the corporate family centrally pool financial accounts? Is there an automated system that transmits financial data to an affiliate? Does an affiliate do a sweep of the mitigated accounts, and if so, how often? Has my company accepted any intracompany loans, and if so what are the terms of repayment? Have any notes been executed, and if so under what terms?

- **Audit/Quality Assurance:** Does the parent require that internal audits be conducted? If so, who conducts them? What information is accessed at my company to complete an internal audit? What safeguards are in place to prevent improper information obtained through an internal audit from being conveyed to the affiliate? What entity performs external and financial audits? If a third party performs external and financial audits, is there a separate engagement letter or contract with the my company?

- **Marketing/Advertising/Business Development:** Are any customer/program details provided to the affiliate for marketing or advertising purposes? Does my company participate in trade shows? If so, do we do so in conjunction with any of our affiliates? Are program/project details provided to the affiliate(s) for business development purposes? Does the TCO or another official review the material for compliance with Export Administration Regulations (EAR) and/or International Traffic in Arms Regulations (ITAR)?

- **Recruiting:** Does my company employ recruitment personnel? If so, to whom do these individuals report? Do the entities share an online recruitment portal? If so, who makes initial candidate cuts? Who drafts and posts job advertisements, and who reviews resumes?

- **Human Resources:** Do affiliate entities assist with or direct the hiring/firing of employees at my company? Does my company employ H.R. personnel? If so, to whom do these individuals report? Does the affiliate assist with legal aspects of H.R. such as Americans with Disabilities Act (ADA) and Equal Employment Opportunity (EEO) dispute resolution or workman's

compensation claims? Does the affiliate audit my company's compliance with corporate policies and state and federal regulations? Does an affiliate assist with employee evaluations at my company? Are salaries and incentives influenced by any affiliate?

- **Procurement:** Does my company use any master corporate contracts held by an affiliate? If an affiliate purchases IT equipment, does the contract let them access the records on those systems? Does my company have the ability to make alternate arrangements for purchasing goods and services?
- **Payroll:** Is employee data traceable to specific customers, contracts or program information?
- **Real Estate:** Who holds the leases or deeds for my company's real estate? If an affiliate owns/leases the property, do they retain a right of entry? If an affiliate owns/leases the property, do they decide who performs maintenance? Is there a system to track all entries onto the premises?
- **Accounts Payable/Receivable:** Is any customer, contract or program identifying information redacted? To what account will payments be made?
- **Training:** Are visit requests and contact reports maintained for training opportunities involving my company and affiliates? Is the training available to all employees or is participation restricted to KMPs or technical positions? Do training opportunities extend for an inordinate amount of time? If training is held at the cleared facility, how is classified and export controlled information discussions are protected from affiliates?

When non-compliance with an approved AOP is found, DSS will take the following actions:

- DSS will issue a letter of noncompliance with the AOP. A suspense date will be set for the company to respond and address all of DSS's concerns.
- If an acceptable response is not promptly received, DSS will require an immediate end to the affiliated operation(s).
- If DSS receives a response within the established timeline, DSS will evaluate steps taken by the company in addressing DSS's concerns and make a determination on whether the affiliated operation(s) may continue.
- DSS may require additional measures to ensure compliance with the FOCI mitigation agreement.
- An amended AOP incorporating the additional security measures may be required.
- **Repeated and systemic non-compliance in this area may jeopardize the status of the facility security clearance.**

CONCLUSION

To reiterate, affiliated operations exist when a FOCI mitigated company leverages services or operations from or with an affiliate; provides such services or operations to an affiliate; shares a third-party service provider or employees with an affiliate; or engages in collaborative commercial arrangements with an affiliate.

The AOP was created to provide FOCI mitigated companies, GSCs, affiliates, and DSS with transparency about the types of interactions and relationships the FOCI mitigated entities have with their affiliates.

Through this transparency, the parties can identify potential risks of unauthorized access to classified and/or sensitive information, undue influence on performance on classified contracts, or inappropriate influence over the management of FOCI companies.

The parties work together to create and implement mitigation measures guaranteeing that the GSC and DSS maintain proper oversight over the affiliated operations.

The AOP should show that the company has taken steps to identify and mitigate all FOCI risks.

FOCI companies should continuously oversee the implementation of the AOP. The company's employee/affiliate interaction at the individual, group, and organizational levels should be evaluated.

Furthermore, when creating leaner organizations through automation, downsizing, or outsourcing, any resulting affiliate interaction and support should be addressed before decisions are made.

With the advancement of technology, FOCI mitigated companies should be evaluated at every level for potential affiliated operations leveraging technologies and related services.

In order for the FSO to evaluate every level of the business he/she must have management support from the GSC and the Board. Including the FSO in senior management meetings and/or Board Meetings will help identify affiliated operations that must be included in the AOP.

Training employees, including senior leadership, to notify the FSO when operations are leveraged will also help identify potential affiliated operations that may need to be included in the company's AOP.

Lastly, affiliated operations usually result in electronic communications and visits between the entities. The FSO can identify

additional services while reviewing electronic communications and visit requests per the ECP and Visitation Policy required by the FOCI mitigation agreement.

The business environment is ever-changing, so the AOP must be a living document that captures and accommodates those changes while fulfilling DSS's requirements.

DSS will maintain its partnership with industry by working diligently to help reconcile a company's goals with DSS's mission, particularly by and through the AOP.

The AOP was a product of DSS's continuous conversations with industry and crafted for industry. DSS looks forward to continuing those conversations going forward.

ACRONYMS & ABBREVIATIONS

AOP Affiliated Operations Plan

EAR Export Administration Regulations

ECP Electronic Communications Plan

FCL Facility Security Clearance

FLP Facility Location Plan

FOCI Foreign Ownership, Control, or Influence

FSO Facility Security Officer

GCA Government Contracting Activity

GSC Government Security Committee

ISR Industrial Security Representative

ITAR International Trafficking in Arms Regulations

NISP National Industrial Security Program

TCO Technology Control Officer

DEFINITIONS

AFFILIATE: An entity within the ownership chain of a mitigated company, but which is itself not subject to a FOCI mitigation agreement; refers to both (a) the Ultimate Parent and (b) each entity that directly or indirectly controls, is directly or indirectly controlled by (other than the mitigated company and its controlled entities), or is directly or indirectly under common control with the Ultimate Parent.

AFFILIATED OPERATIONS: A business or operational relationship between a mitigated company and an affiliate, to include any internal policy, process, or procedure that could give an affiliate financial or operational leverage over the mitigated company.

ARMS-LENGTH TRANSACTION: Business deals in which the buyer and seller act independently and on an equal footing.

CONTROLLED ENTITY: a corporation in which a mitigated company owns a controlling interest, either directly or indirectly through the mitigated company's ownership interest in intermediate companies as determined by DSS.

EXPORT ADMINISTRATION REGULATIONS (EAR): The Export Administration Regulations (EAR), Title 15, sections 730-774 of the Code of Federal Regulations (CFR), means the regulations promulgated and implemented by the Department of Commerce that regulate the export of goods and related technology identified on the Commodity Control List (CCl), Title 15 CFR 774, Supp. 1. Goods and technology on the CCl are not inherently military in nature; they are primarily and inherently commercial or potentially commercial in nature.

EXPORT CONTROLLED INFORMATION: Information that is the subject of laws, policies, and regulations that govern the export of sensitive items for a country or company.

INFORMATION: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

INTERNATIONAL TRAFFICKING IN ARMS REGULATIONS (ITAR): The regulations promulgated and implemented by the Department of State (DoS) that control the export of articles, services, and related data that are inherently military in nature, as determined by DoS.

MITIGATED COMPANY: An entity bound by a FOCI mitigation instrument; refers both to signatory facilities and all subsidiaries and controlled entities thereof.