

National Security Alert

Considerations for FOCI-Mitigated Companies: Leveraging ERP Systems

Many global corporate groups deploy Enterprise Resource Planning (ERP) systems to manage the business operations of their subsidiaries and business lines, improve efficiencies and reduce costs. Foreign-owned US companies holding facility security clearances and operating under foreign ownership, control or influence (FOCI) mitigation arrangements face national-security policy challenges in participating in their group's ERP systems. ERP issues most frequently arise in the context of cleared companies with majority FOCI operating under Special Security Agreements (SSA) or Proxy Agreements, though ERP can also be relevant to companies operating under Security Control Agreements and (although not frequently used) Voting Trust Agreements. The US Department of Defense's Defense Security Service (DSS) generally prohibits standard information technology (IT) connections between such FOCI-mitigated companies and their non-mitigated parents and affiliates (Affiliates). Nonetheless, in certain cases—and subject to additional security measures—DSS has permitted FOCI-mitigated companies to participate in corporate group ERP systems. This alert discusses key issues related to a FOCI-mitigated company's involvement with its corporate group's ERP systems, as well as measures that can be implemented to maximize the chances of such arrangements being approved.

ERP systems are business-management software suites that companies can utilize to collect and manage business data to improve efficiencies within the corporate group's operations. These suites can cover numerous applications, including, among others, finance, human resources, sales and marketing, and project planning and execution.

In general, DSS requires the operations and management of FOCI-mitigated companies and their Affiliates to be separate, particularly for companies operating under SSAs or Proxy Agreements. Consistent with this and DSS's focus on IT-security concerns, DSS has restricted network connections between FOCI-mitigated companies and their Affiliates. There are, however, structures and mitigation methods that DSS might accept to enable FOCI-mitigated companies to participate in group-wide ERP systems. Please note that since SSAs are generally less restrictive than Proxy Agreements, DSS may be more flexible in approving ERP participation for companies operating under SSAs than Proxy Agreements.

DSS reviews proposed network connections and contemplated affiliated operations (e.g., affiliated services, shared third-party services) on a case-by-case basis, taking into account the specific FOCI factors and other considerations related to the FOCI-mitigated company and the contemplated interactions. Electronic communications are addressed in an Electronic Communications Plan (ECP), which presents a profile of the FOCI-mitigated company's network, including how it is protected from outsiders and Affiliates. Affiliated operations are addressed in an Affiliated Operations Plan (AOP).

There are numerous factors that need to be considered in addressing a given FOCI-mitigated company's contemplated ERP participation, including details pertaining to the company's network configuration and desired ERP links, as well as certain tailored mitigation measures. The following are some of the specific measures and mitigation steps that in our experience have helped provide an avenue for FOCI-mitigated companies to participate in their group's ERP systems:

- Network connections to the ERP systems must be configured so that information pertaining to the FOCI-mitigated company is "pushed" (i.e., affirmatively provided by the FOCI-mitigated company) to an Affiliate. Affiliates must be prohibited from "pulling" (i.e., autonomously accessing) information from the FOCI-mitigated company's network. Potential solutions to satisfy the DSS "push-pull" policy include:
 - having the ERP systems hosted by a third-party US company located within the United States; or
 - the FOCI-mitigated company establishing a stand-alone connection to the Affiliate network; i.e., a one-way connection that is separate from the FOCI-mitigated company's main network and links only to the Affiliate's network.
- Generally speaking, all business-related information may be released by the FOCI-mitigated company to the Affiliates' ERP systems as long as the data does not contain classified information, export-controlled information, operations-security information or certain unclassified information related to classified contracts. The SSA and Proxy Agreement do not prohibit the release of business information from a FOCI-mitigated company to an Affiliate, and the Proxy Agreement expressly authorizes the release of financial information, provided DSS approves the formats for such reporting.

- The Government Security Committee (GSC) should approve the formats used for reporting and submitting data via the ERP systems. Typically, there is no need for the GSC to approve routine submissions after approving the formats, but it should do spot checks as part of regular quarterly monitoring.
- It may be appropriate to have an independent third party conduct audits regularly to ensure compliance with the approved arrangement and confirm that the security requirements are being met to protect sensitive information. The GSC should approve the scope of audits and approve—and redact as necessary—any audit reports before they are provided to Affiliates.
- The details of the contemplated arrangement, both operationally and from a technical perspective, as well as risk-mitigation measures, should be detailed in both the FOCI-mitigated company's ECP and its AOP.

The specific details of a given FOCI-mitigated company's contemplated ERP participation should be carefully planned with the company and its relevant Affiliates and be supported by the GSC before being presented to DSS. Although there may be some restrictions on the nature and extent of ERP utilization, with proper planning and coordination, ERP systems can be a viable business tool for most FOCI-mitigated companies.

Contact Us

For additional information about ERP participation for FOCI-mitigated companies or other ECP- or AOP-related matters, or to learn more about the FOCI-mitigation process or Kaye Scholer's National Security/CFIUS practice, please contact any of the following:

Farhad Jalinous

+1 202 682 3581

farhad.jalinous@kayescholer.com

Karalyn Mildorf

+1 202 682 3547

karalyn.mildorf@kayescholer.com

Keith Schomig

+1 202 682 3522

keith.schomig@kayescholer.com

Norman Pashoian

+ 1 202 682 3562

norman.pashoian@kayescholer.com

• Chicago
• Frankfurt
• London

• Los Angeles
• New York
• Shanghai

• Silicon Valley
• Washington, DC
• West Palm Beach

KAYE | SCHOLER