CASE STUDY

ISI

TWO REQUIREMENTS, ONE PROJECT:

A FOCI PROBLEM THAT NEEDED AN IT SOLUTION

CLIENT PROFILE

A U.S. subsidiary of a European-based company seeking to win defense and federal contracts, operating in a cloud environment with an existing Foreign Ownership, Control, or Influence (FOCI) mitigation agreement already in place.

CAUGHT BETWEEN TWO TECHNICAL WORLDS

The subsidiary was caught between the environment it had and the one it urgently needed. Its Microsoft tenant remained tied to its parent company, creating a structural barrier to pursuing DoW work and satisfying the terms of its FOCI mitigation agreement.

Any path forward needed to do more than resolve that immediate conflict. The organization required a solution that would:

- Satisfy the FOCI mitigation agreement as written
- Position the subsidiary to support CUI work as its DoW business matured
- Preserve the ability for users on the new commercial tenant to collaborate with the parent company's tenant on projects where that collaboration was appropriate and permitted

The stakes extended beyond the subsidiary itself. Any proposed solution had to satisfy the parent company's board of directors; which meant arming the subsidiary's internal champion with a technical solution robust enough to build the case and win board-level approval.

THREE OBSTACLES, ONE NARROW WINDOW

1

A self-inspection was imminent.

With a formal DCSA review on the horizon, the subsidiary needed its FOCI mitigation documentation, an Electronic Communications Plan (ECP) and Technology Control Plan (TCP), properly implemented, not just documented.

2

Disruption was not an option.

The subsidiary needed a compliant environment built within weeks, without cutting off staff from other in-progress projects outside the agreement's scope.

3

The market had no good answer.

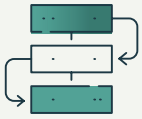
Most MSSPs lack the FOCI expertise to interpret mitigation instruments. Most security advisory firms lack the IT capability to build out a new tenant. The subsidiary needed both and couldn't afford two vendors talking past each other.

LISTEN FIRST, BUILD SECOND: HOW ISI APPROACHED THE CHALLENGE

Before proposing anything, ISI brought together its Managed Security Services (MSS) and Managed IT, Cybersecurity, and Compliance teams under a single engagement to create one clear path, eliminating the gap that leaves most defense-bound subsidiaries stranded between compliance advisors and infrastructure teams.

ISI's team then held multiple working sessions with company leadership to deeply understand the FOCI mitigation plan, the parent relationship, and the operational constraints that any solution would have to respect.

THE RESULT



01

ISI proposed a phased plan built for real-world constraints: review the FOCI agreement to set the initial boundary aligned with the ECP and TCP; stand up a new commercial tenant for the subsidiary, fully separated from the parent; and build a GCCH enclave for future CUI work, sequenced to proceed only after DCSA approval.

02

FOCI expertise driving technical execution. ISI's internal FOCI knowledge shaped every infrastructure decision, ensuring the new environment satisfied the mitigation agreement while simultaneously building toward all 110 controls and 320 objectives of NIST 800-171, as required under DFARS 252.204-7012.

03

A solution three stakeholders could say yes to. The final plan was structured to satisfy the subsidiary's operational goals, the parent company's board, and the terms of the FOCI agreement, a balance most single-discipline vendors would not have known to pursue

04

Armed the internal champion, not just the plan. ISI met regularly with the subsidiary's senior management official leading the project, translating the technical solution into the business case its parent company's board needed to hear, and equipping them to make that case with confidence.

COMPLIANT, CONNECTED, AND CONTRACT-READY

The subsidiary cleared its self-inspection and formal DCSA review with confidence, positioned to begin pursuing defense and federal contracts as intended.

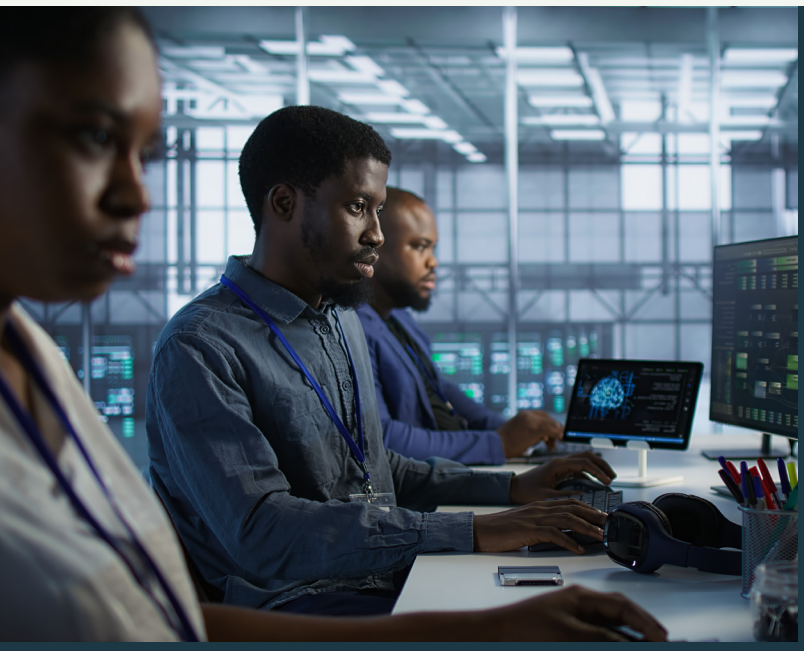
Throughout the transition, staff never lost the ability to collaborate with the parent company on non-defense work; **the new commercial environment preserved that connection exactly as leadership required**, without compromising the separation the FOCI agreement demanded.

BUSINESS OUTCOMES

- **Passed DCSA self-inspection** with FOCI mitigation documentation fully implemented, not just filed
- **Preserved cross-tenant collaboration** on non-defense projects throughout the transition, avoiding operational disruption
- **Resolved FOCI compliance, tenant separation, and DFARS 7012 readiness** in a single coordinated engagement, faster and cheaper than a multi-vendor approach

TECHNICAL OUTCOMES

- **Stood up a new commercial Microsoft tenant**, fully separated from the parent company's environment
- **Built infrastructure aligned to the ECP and TCP** boundaries defined during the FOCI agreement review
- **Positioned the environment to meet all 110 controls of NIST 800-171**, as required under DFARS 252.204-7012
- **Sequenced a GCCH enclave build** to follow immediately on DCSA approval, giving the subsidiary a clear path to CUI-eligible work



KEY TAKEAWAY

For defense-bound subsidiaries navigating FOCI, the gap between compliance knowledge and IT execution is where opportunities are lost. ISI closed that gap here, and when one partner holds both the FOCI expertise and the technical capability to act on it, what looks like a tangle of competing requirements becomes one clear path forward.