OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Report on Common Sensitive Compartmented Information Facility

September 2020

Table of Contents

(U) EXECUTIVE SUMMARY

The IAA Joint Explanatory Statement of the Fiscal Year 2020 Intelligence Authorization Act directed the Office of the Director of National Intelligence (ODNI) to deliver a briefing on the following topics:

1. Steps necessary to establish new "Common SCIFs" (sensitive compartmented information facility) in areas of high demand.
2. What approaches allow SCIF spaces to be certified and accredited outside of a traditional contractual arrangement?
3. Analysis of the advantages and disadvantages of issuing Department of Defense (DoD) Contract Security Specification form (DD Form 254) to ''facilities,'' as opposed to ''contracts.''
4. Options for classified co-use and shared workspace environments such as innovation, incubation, catalyst, and accelerator environments.
5. Pros and cons for public-, private-, government-, or combination-owned classified neutral facilities.
6. Any other opportunities to support those without ownership of a SCIF effective access to a neutral SCIF.

(U) INTRODUCTION

As requested, the staff of the National Counterintelligence and Security Center (NCSC), which oversees physical security policy for the Intelligence Community (IC), briefed committee staff on these issues on 25 September 2019. The ODNI offers this report as a follow-up to that briefing, and we would be pleased to provide additional information if requested.

Before addressing the specific questions outlined in this request, it is important to note some overarching points. While the terminology used in the questions varies, the spirit underlying these questions seeks additional flexibility and creativity to allow industry to contribute to national security work. Within the IC, we have been wrestling with these topics for some time. The challenge has been to maintain reciprocity by applying proven common standards, while acknowledging that the workplace is shifting. Such increased flexibility is one of the hallmarks of our Trusted Workforce 2.0 initiative to reform personnel security vetting. We intend also to follow that same spirit in the physical security realm. Given the significant backlog of personnel security clearances and the undeniable demand signal for change across that enterprise, we prioritized our work focusing a great deal of attention on reforming personnel vetting.

The ODNI also considered balancing the cost against the convenience of any changes to our physical security policy would bring, as they pertain to industry. Policy changes require working across the whole of government to ensure their success, but such work is necessarily deliberative in nature and therefore not accomplished quickly. This thoughtfulness is important because changes will drive additional resource requirements that the U.S. Government must plan for years in advance of becoming reality. We must therefore be clear about what the U.S. Government's role vis-à-vis private industry is when it comes to classified work to ensure both a level playing field and the most effective national security apparatus possible. Additionally, policy changes should always be consistent with guidance calling for the IC to take an analytical risk management approach, "assessing threats against vulnerabilities and implementing security enhancements to achieve the protection of information and resources at acceptable levels of risk and cost" (IC Standard 705-1).

We welcome further exploration of these issues in due course. Coupled with our earlier briefing, this response provides some additional considerations regarding the questions posed. This includes insight gained through our oversight role, engagement with the IC Security Directors, and a review of various laws and regulations, including the Federal Acquisition Regulation (FAR) space utilization requirements, and information and industrial security requirements, including protections for company proprietary information and need-to-know.

(U) STEPS NECESSARY TO ESTABLISH NEW "COMMON SCIFS" IN AREAS OF HIGH DEMAND:

The IC often establishes new SCIFs for both government and industry, depending on mission needs. NCSC executes the ODNI's responsibility to develop and oversee policy for new and existing SCIFs, including ensuring compliance with IC SCIF standards and the accreditation process. Although the DNI delegated the responsibility of protecting SCI to the Cognizant Security Authority (CSA) via the IC element head, the ODNI is responsible for setting SCIF policy standards to enable reciprocal use of SCIFs.

The Physical and Technical Security Working Group (PTSEWG) develops SCIF policy and chairs an interagency group comprised of physical and technical security subject matter experts from the IC, Non-Title 50 organizations, and the Industrial Security Working Group (ISWG). The PTSEWG meets monthly, discussing SCIF management issues and deliberating on revisions of technical standards.

There are several sub-working groups under the PTSEWG responsible for technical expertise in such topics as intrusion detection systems, doors and locks, electronic medical devices, and SCIF training. These sub-groups develop changes to physical security standards, which are then briefed to the main PTSEWG for concurrence.

Proposed policy changes are sent to the ODNI General Counsel, policy process experts, and IC security policy personnel for review and edit. Eventually, depending upon the level of the proposed policy, it is reviewed and, if deemed appropriate, approved by either Director, NCSC or the DNI.

It is important to note that any SCIF, including so called "Common SCIFs," must have a U.S. Government sponsoring agency. This is a challenge, as we discuss later. However, while policy does not address "Common SCIFs" per se, there is a provision in IC Standard 705-2 allowing for co-use agreements (called joint-use if the hosting agency's information technology systems are used) so other organizations may use SCIF spaces as needed. In this model, the host and proposed tenant sign a Memorandum of Agreement to document the relationship and the tenant accepts the host's SCIF accreditation parameters (e.g. open storage vs. closed storage or discussion vs. non-discussion). The tenant bears the cost of any modifications required to meet their unique needs. It is important to note that contractor SCIFs may be co-used provided they are sponsored by a Government agency that the vendor supports with classified work. The Government, as the responsible party for overall protection of the classified government information housed or worked on at the vendor site, must approve the SCIF at the vendor location, which is under its cognizance. This model has been enacted thousands of times and works well.

NCSC also maintains the SCIF Repository, which provides insight into thousands of SCIF records, from both Government and industry, to include their location, sponsoring agency, co-use agreements, size, and other key elements. This database is available to accreditors and physical security practitioners and is particularly useful in situations of accelerated need for SCIFs in certain geographic locations.

We conclude that the liberal use of co-use agreements, coupled with the information available to U.S. Government accreditors and physical security practitioners, provides Government and industry with appropriate opportunity and flexibility on SCIF access.

(U) WHAT APPROACHES ALLOW SCIF SPACES TO BE CERTIFIED AND ACCREDITED OUTSIDE OF A TRADITIONAL CONTRACTUAL ARRANGEMENT?

All SCIF spaces employed by Government, academic, and commercial entities are established following the same accreditation process and are subject to the same technical specifications. This common approach is necessary to permit reciprocity and ensure the appropriate safeguarding of classified material. Security requirements and guidance, including access and safeguarding requirements, are provided to contractors and academia by the Contract Security Classification Specification portion of the Federal Acquisition Regulation (FAR) and are carried out by completing the DD Form 254, which is required by the FAR for all classified contracts.

If we shifted to a system whereby commercial SCIFs were certified and accredited outside of a traditional contractual arrangement, several issues would arise. First, the reason that SCIF certification and accreditation for industry is tied to a specific contract is that work done under each contract is different, so security professionals need to review the safeguards required for each specific situation. The security measures appropriate for the information supporting one agency's contract may be insufficient for another, or there may be different classified information technology system requirements. Second, government resources are necessary to assess the facility for certification and accreditation and should not be expended in the absence of certification and approval from a government agency that such space is required. Otherwise, we are in danger of giving an unfair competitive advantage to one company over others by essentially granting them classified workspace for no specific reason.

While this details the current approach to SCIF management for industrial SCIFs, the ODNI remains open to considering alternative approaches, so long as those alternatives are based on a certified need to the Government.

(U) ANALYSIS OF THE ADVANTAGES AND DISADVANTAGES OF ISSUING DEPARTMENT OF DEFENSE CONTRACT SECURITY SPECIFICATIONS (DD FORM 254S) TO "FACILITIES," AS OPPOSED TO "CONTRACTS".

As noted, current industrial security policy is driven by two main documents, the FAR and the National Industrial Security Program Operating Manual (NISPOM). Both outline a construct that in essence differentiates between the security requirements necessary to work on a specific contract (the DD Form 254) and the requirements for a facility in which classified work for the government occurs (the Facility Clearance). Any company wishing to perform work on a classified U.S. Government contract must comply with both requirements.

The Government uses the DD Form 254 to convey specific security requirements to contractors when contract performance requires access to classified information. Prime contractors also use the DD Form 254 to convey security requirements to subcontractors that require access to classified information to perform on a subcontract. Subcontractors may also use the DD Form 254 if access to classified information is required to convey security requirements to additional subcontractors. The DD Form 254 must be updated every two years.

The DD Form 254s are critical for each classified contract because the security requirements pertaining to that work are unique. Even if the same company performs work on two different contracts in the same facility, the security parameters may well be different to adequately protect the work. For example, one may permit open storage, or require access to a specific classified compartment, while the other does not. Those distinctions are enumerated in the DD Form 254 and would be lost if we only relied upon the Facility Clearance.

We are aware that industry views the DD Form 254 as onerous and would prefer a streamlined process. To that end, in 2019, the government changed the submission process for the existing DD Form 254 to enable businesses to submit an electronic form once, instead of repeated paper submissions. This change was well received. Despite the sentiment in some quarters for changing the DD Form 254 to address facilities rather than contracts, the ODNI maintains that such a move would jeopardize the security of classified work being done by our industrial partners.

(U) OPTIONS FOR CLASSIFIED CO-USE AND SHARED WORKSPACE ENVIRONMENTS SUCH AS INNOVATION, INCUBATION, CATALYST, AND ACCELERATOR ENVIRONMENTS:

As stated in Response 1.

(U) PROS AND CONS FOR PUBLIC, PRIVATE, GOVERNMENT, OR COMBINATION OWNED CLASSIFIED NEUTRAL FACILITIES:

The appeal of multi-use classified space is apparent. As we reshape the national security workforce, we are thinking about the working environment it requires. This is part of the ODNI-led “Right, Trusted, Agile Workforce” initiative. We see the synergy gained when different entities are co-located and fully appreciate the transportation challenges in places like the Washington DC metro region where access to a geographically-desirable SCIF can be an advantage.

Among the challenges would be the prohibitive costs for security, if the government were to maintain a SCIF that is available for only periodic use by multiple users. Meeting security requirements for individual contracts/efforts for one agency could adversely affect co-use arrangements with other agencies. An example would be the government sponsor of such a facility needing to spend additional funds for the different levels of required physical and access protection for the SCIF or Compartmented Areas due to the different programs or Special Access Programs therein. Complicating matters is the possibility of other agencies’ IT systems used within that facility, which would represent a significant vulnerability if not mitigated with additional protective measures. IC elements’ budgets do not have the leeway to build and secure “neutral” or “common” SCIFs beyond what they require for their current use.

Additionally, there are multiple policy restrictions in place that would have to be surmounted. Construction of “neutral” or “common” SCIFs would conflict with multiple acquisition, space management, and information protection statutes and regulations. While the need for policy changes alone should not prevent the exploration of ideas, the extended time and costs required to change such policies and guidelines must be taken into account. We do not conclude such an alternative approach is needed at this time as current policies and procedures already maximize industrial SCIF reciprocity and co-utilization, while providing requisite security protection to sensitive compartmented information.

(U) ANY OTHER OPPORTUNITIES TO SUPPORT THOSE WITHOUT OWNERSHIP OF A SCIF EFFECTIVE ACCESS TO A NEUTRAL SCIF

The IC and industry follow the FAR and NISPOM process for all requests for SCIF access and construction of new SCIFs. While we are sensitive to the demand signal from certain industry partners to revisit our SCIF policies, for the reasons enumerated previously, we do not propose making wholesale changes to current practices at this time. However, we stand ready to assist by further engaging with the IC Security Directors and the PTSEWG on this topic and its future possibilities.