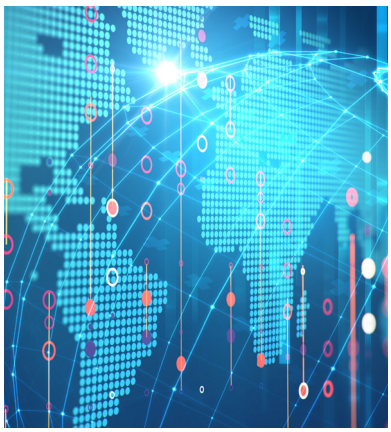
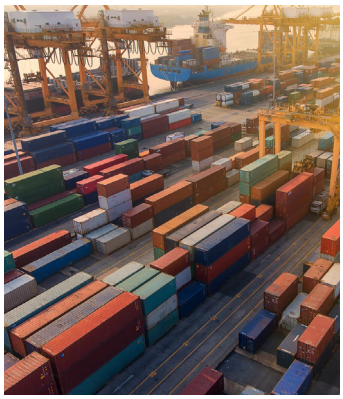
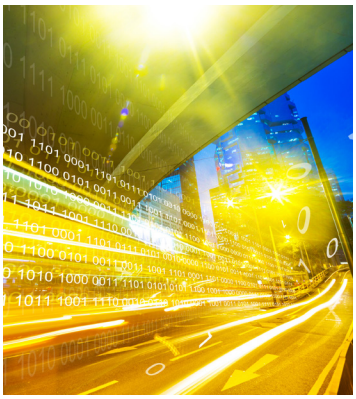
WHITE PAPER:

Recent Department of Defense Guidance on Cybersecurity Requirements and Related Export Control Issues







Akin Gump
STRAUSS HAUER & FELD LLP

RECENT DEPARTMENT OF DEFENSE GUIDANCE ON CYBERSECURITY REQUIREMENTS AND RELATED EXPORT CONTROL ISSUES

The U.S. Department of Defense (DoD) recently issued two sets of guidance regarding Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (the -7012 Clause). The most recent guidance was attached to an April 24, 2018 notice and request for comment titled "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented." 83 Fed. Reg. 17,807 (the April 24 Guidance). The second set of guidance consists of updated Frequently Asked Questions that DoD issued on April 2, 2018 (the Updated FAQs). This White Paper examines the impact of the April 24 Guidance and the Updated FAQs on the role of contractor System Security Plans (SSPs) and Plans of Action and Milestones (POAMs) in source selection and contract performance, the proper interpretation of particular National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 requirements, and the potential impact of the -7012 Clause safeguarding and reporting requirements on export-controlled information resident in contractor information systems.

1. Evaluation of SSPs and POAMs During Source Selection and Contract Performance

As we previously explained in this post, the -7012 Clause requires contractors to provide "adequate security" for covered defense information (CDI) when it is stored, processed or transmitted by information systems operated by, or on behalf of, the contractor or when performance of the DoD contract involves operationally critical support. The -7012 Clause states that adequate security requires, at a minimum, that information systems on which CDI is processed, stored, or transmitted comply with the security requirements of NIST SP 800-171. Contractors subject to the -7012 Clause are required to flow that clause down to subcontractors at all tiers, with the exception of Commercial Off the Shelf (COTS) item subcontractors, that have, or will have, CDI on their information systems or that will perform operationally critical support.

NIST SP 800-171 Requirement 3.12.4 requires the organization to "[d]evelop, document, and periodically update [SSPs] that describe system boundaries, system requirements of operation, how security requirements are implemented, and the relationships with or connections to other systems." DoD expects SSPs to describe how the NIST SP 800-171 security requirements are met or how the contractor plans to meet any security requirements that have not been met. In addition, NIST SP 800-171 requires organizations to develop and implement POAMs that are designed "to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems." DoD expects POAMs to describe how any unimplemented security requirements will be met and how any unmet requirements or requirements with identified deficiencies will be mitigated.

Previous DoD guidance stated that procuring agencies were authorized to request and evaluate offerors' SSPs and POAMs in the course of making procurement decisions. The April 24 Guidance provides more detail on the use of SSPs and POAMs in that regard and in monitoring contract performance after a contract is awarded.

The April 24 Guidance includes a draft document titled "DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented." This document is intended to facilitate agencies' review and understanding of the risks that any offeror's or contractor's failure to meet a particular security requirement may have on the offeror's or contractor's information system, and to assist in prioritizing the implementation of security requirements not yet implemented. To that end, the draft document establishes "DoD value" metrics that assign priority rankings to each security requirement. These rankings, like the NIST SP 800-171 requirements themselves, are based upon the security requirements of NIST SP 800-53 and range from 1 to 5, with 1 representing the lowest impact on an information system and thus being of the lowest priority for implementation. The draft document cautions that these metrics are "not to be used to assess implemented security requirements, nor to compare or score a company's approach to implementing a security requirement."

The draft document is accompanied by a matrix titled "Assessing the State of a Contractor's Internal Information System in a Procurement Action." This matrix illustrates various ways in which DoD may assess SSPs and POAMs in the course of source selection decisions and contract performance. The matrix is structured around four "objectives": (1) evaluation or assessment of a contractor's implementation of NIST SP 800-171 at the time of source selection; (2) evaluation of protections implemented by a contractor that go beyond the NIST SP 800-171 security requirements at the time of source selection; (3) assessment of implementation of NIST SP 800-171 requirements after contract award and monitoring of compliance with the requirements; and (4) confirmation of a contractor's self-certification with the -7012 Clause and NIST SP 800-171. Each objective is accompanied by clauses and additional information that the source selection authority must include in a solicitation or Request for Proposals, an explanation of how the source selection authority should evaluate an offeror's compliance with specific requirements, and clauses and documents that must be included or incorporated in any contract that is awarded.

The April 24 Guidance presents many practical challenges for offerors. To begin with, the new guidance will impact how offerors draft and compile information for their proposals. Offerors will need to ensure that their SSPs and POAMs are accurate, complete and proposal-ready. Furthermore, offerors may have to obtain SSPs and POAMs from teaming members and other proposed subcontractors for proposal submission. To the extent that teaming partners or potential subcontractors even have SSPs or POAMs, they are likely to regard them as proprietary and confidential and will want to limit their distribution. Second, they may be hesitant to share their SSPs and POAMs with the offeror or the government out of concern that these documents would reveal weaknesses in their systems or create compliance issues. Finally, team partners or potential subcontractors may be concerned that the offeror might use their SSPs and POAMs to its advantage in a later procurement where the teaming partners or potential subcontractors are the offeror's competitors. Each of these concerns would likely be heightened in the case of foreign teaming partners and suppliers and potential subcontractors that are small or medium-sized businesses.

The April 24 Guidance is also likely to serve as a basis for bid protests, particularly in the short term as DoD source selection authorities grapple with how best to implement it. In the pre-award phase, an offeror may have the opportunity to protest if it believes that the terms of a solicitation are contrary to the guidance. Post-award, a disappointed offeror may have the opportunity to protest the agency's evaluation of SSPs and POAMs. Another potential issue for post-award protests is the disclosure of SSPs and POAMs in the administrative record to the extent that they constitute or contain CDI. For example, it is unclear exactly what CDI safeguarding requirements would apply to a law firm representing a protesting party in order to receive copies of the awardee's SSP or POAMs. To date, we have not seen any guidance from the Government Accountability Office on this issue.

Finally, the fact that the April 24 Guidance requires SSPs and POAMs to be assessed in connection with the award of a DoD contract means that a contractor could face allegations of potential "fraudulent inducement" False Claims Act liability if its proposal misrepresents its current compliance with security requirements and/or its intentions or plans with respect to unmet security requirements. Of course, under *Universal Health Services, Inc. v. United States ex rel. Escobar,* 136 S. Ct. 1989 (2016), the U.S. Department of Justice or a *qui tam* relator would have to show that the offeror's false or misleading

representations about its compliance with security requirements were material to the agency's decision to award the contract to the offeror.

Comments on the April 24 Guidance are due by May 31, 2018.

2. NIST Security Requirements Addressed/Altered in Updated FAQs

The following discussion is intended to serve as a high-level summary of some of the most significant changes and revisions reflected in the Updated FAQs.

a. SSPs/Compliance with NIST SP 800-171

As something of a corollary to the April 24 Guidance discussed above, the Updated FAQs discuss SSPs and POAMs and their role in contractor selection and contract administration. DoD's response to FAQ 53 states that SSPs "provide[] a mechanism to address, as part of the requiring activities overall risk management decision, situations in which all of the NIST SP 800-171 security requirements are not fully implemented on the covered contractor's information system." DoD's response to FAQ 91 states that "requiring activities may utilize the [SSPs] and associated [POAMs] in a variety of ways in the contract formation/administration process in order to obtain the level of security that they require." Response to FAQ 91 goes on to establish that these include, but are not limited to:

- Require that proposals identify any NIST SP 800-171 security requirements not implemented at the time of award and include associated plans of action for implementation. Implementation of NIST SP 800-171, as documented in the [SSP] or otherwise, would be considered as part of the source selection process. Proposal instructions and corresponding evaluation specifics of how implementation of NIST SP 800-171 will be used by the DoD to determine whether or not it is acceptable or unacceptable to process, store, or transmit covered defense information on a system hosted by the offeror must be detailed in sections L and M of the solicitation as well as the Source Selection Plan. This scenario is outside of the scope of [the -7012 Clause].

- Identify in the solicitation that all security requirements in NIST SP 800-171 must be implemented at the time of award. Planned or partial implementations would generally not be allowed, with the exception of any enduring exceptions to the requirements to accommodate special circumstances (*e.g.,* medical devices), or any individual, isolated or temporary deficiencies. This scenario is outside of the scope of [the -7012 Clause].

- The contractor will self-attest to be compliant with [the -7012 Clause], to include implementation of NIST SP 800-171 (which allows for planned implementation of some requirements if documented in the [SSP] and associated plans of action), by signing the contract at the time of award. No additional conditions beyond [the -7012 Clause] are imposed.

DoD's response to FAQ 50 states that DoD requiring activities "should restrict their security requirements to [the -7012 Clause] and NIST SP 800-171 unless there is a specific need to increase security above the 'Moderate' impact level." If the DoD requiring activity expects full implementation of all NIST SP 800-171 requirements at the time of contract award, it should specifically identify such requirement in the solicitation. *See* Response to FAQ 53. Furthermore, if an offeror meets the requirements of NIST SP 800-171, the DoD requiring activity should not use the evaluation/source selection process to define the acceptability of how the contractor meets those requirements. *See* Response to FAQ 55.

FAQ 92 asks whether there is a "prescribed format/level of specificity" for an SSP. DoD's response states:

> No. Footnote 26 to NIST SP 800-171 Security Requirement 3.12.4 states that, "There is no prescribed format or specified level of detail for system security plans. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans." Additionally, Chapter 3 of NIST SP 800-171, Revision 1 states that, "Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format."

Similarly, DoD's response to FAQ 50 states that DoD components "should not intrude into the operations or management of the contractor's internal IT system by specifying the content and format of the system security plans and plans of action that address deficiencies, requiring any specific method for validating and assessing the system, or specifying the parameters of security requirements."

Finally, DoD's response to FAQ 18 states that, in circumstances where SSPs and POAMs are used to assess the risks in awarding a contract to a particular company, the agency may include in the contract a provision to review the company's progress in implementing its POAMs.

b. <u>Significant NIST Requirements Addressed in the Updated FAQs</u>

The Updated FAQs provide further insight into DoD's interpretation of the well-known NIST 800-171 requirement for multifactor authentication, Requirement 3.5.3. For example, DoD edited the response to FAQ 74 (formerly numbered FAQ 41) to set forth definitions of "Local Access," "Network Access" and "Non-Privileged User." The responses to FAQs 74 and 77 also clarify that, except under certain circumstances, multifactor authentication is not required to access mobile devices like smartphones or tablets, even if those devices contain CDI (although CDI on mobile devices must be encrypted and the encryption module Federal Information Processing Standard (FIPS)-validated, *see* FAQ 78). However, if the mobile device is used to access a contractor information system containing CDI, the system has to provide the capability for multifactor authentication for access by the device, which would be entered via the device (*e.g.*, use of a one-time password device).

The Updated FAQs also provide additional information relating to encryption, another significant NIST security requirement. For example, the response to FAQ 98 clarifies that, with respect to controlled unclassified information (CUI) that is at rest in any nonmobile device or data center and protected by other logical or physical methods, encryption is an option, but not a requirement.

FAQ 68 addresses the NIST security requirements regarding FIPS-validated cryptography and whether it is sufficient if the algorithm is FIPS approved. DoD's response states that:

> Simply using an approved algorithm (*e.g.*, FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at [http://csrc.nist.gov/groups/STM/cmvp/] and [http://csrc.nist.gov/groups/STM/cmvp/validation.html].

FAQ 94 asks whether encryption is required by NIST Requirement 3.13.8 "for a Multiprotocol Label Switching (MPLS) private network (thus an extension of a local network) [that] is multi-tenant protected by [virtual LANS]." DoD's response states that "encryption, though preferred, is not required if using common-carrier provided MPLS, as the MPLS separation provides sufficient protection without encryption."

FAQ 95 asks whether Transport Layer Security (TLS) can be used to protect CDI during transmission over the Internet. DoD's response states that:

> Yes, TLS can be used. The current version of TLS (TLS 1.2) is preferred. If earlier versions must be used to interact with certain organizations, the servers shall not support Secure Sockets Layer (SSL) version 3.0 or earlier. The cryptographic module used by the server and client must be a FIPS 140-validated cryptographic module. All cryptographic algorithms that are included in the configured cipher suites must be within the scope of the validation, as well as the random number generator. For further information see NIST SP 800-52, Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014.

Finally, with respect to the marking of media with CUI markings and distribution limitations per NIST SP 800-171 Requirement 3.8.4, DoD's response to FAQ 86 clarifies that this requirement only applies to CDI and that it does not apply to information provided by, or developed for, non-DoD organizations. It further states that "guidance on marking media, along with other materials, should be addressed separately in the contract and is derived from DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI)."

c. Cloud Computing-Specific Updated FAQs

The Updated FAQs also touch on Federal Risk and Authorization Management Program (FedRAMP) equivalency and certification for cloud providers. The response to FAQ 105 explains that the -7012 Clause does not mandate that a contractor use a cloud services provider that is specifically FedRAMP approved; rather, the -7012 Clause requires a contractor to ensure that the cloud services provided meet those same requirements. With respect to the requirement that cloud services be at least equivalent to "FedRAMP moderate" standards versus NIST SP 800-171 standards, the Updated FAQs suggest that

DoD implemented that requirement because it does not believe that the NIST standards go far enough in securing information stored in the cloud. Instead, DoD requires compliance with FedRAMP moderate standards because they were developed with those additional security measures in mind. The Updated FAQs also note that FedRAMP moderate-level cloud services are well-established and offered by many providers, implying that DoD believes that a contractor should not have difficulty securing services that meet those requirements.

3. Potential Implications of Updated FAQs for ITAR- and EAR-Controlled Information

Among the Updated FAQs are FAQs 25 and 26, which contain important applications of the -7012 Clause to certain export controlled-information—as described in the CUI registry[1] and incorporated into the definition of CDI—and systems that store, transmit or process it. Specifically, these FAQs state, without qualification, that export-controlled information that is "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of [a DoD] contract" qualifies as CDI and must be protected accordingly. As explained below, this interpretation carries potentially broad implications for companies who use pre-existing technical data or technology in the course of their performance on a DoD contract, as well as for foreign suppliers or subcontractors who may possess such data outside the context of a DoD contract or subcontract.

U.S. export control laws generally include the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120–130, administered by the Department of State's Directorate of Defense Trade Controls (DDTC), and the Export Administration Regulations (EAR), 15 C.F.R. §§ 730–774, administered by the Department of Commerce's Bureau of Industry and Security (BIS). Broadly speaking, these regulations prohibit the movement or provision of controlled goods and services outside the United States and to unauthorized non-U.S. persons. In addition, the regulations control the flow of data and information (*i.e.*, "technical data" under the ITAR and "technology" under the EAR) associated with such goods and services. Finally, these regimes prohibit the "release" of information (*i.e.*, through visual or other inspection by, or an oral or written exchange with, unauthorized foreign persons in the United States or abroad).

Although access controls and other information security principles are unquestionably fundamental to ITAR and EAR compliance, neither framework mandates (with some exceptions for cloud computing) specific security standards such as those prescribed by the -7012 Clause. More importantly, the ITAR and EAR do not impose affirmative obligations to report mere network intrusions, absent a triggering export or other release of information. *See, e.g.*, 22 C.F.R. § 126.1(e)(1) (mandating DDTC notification in the event that ITAR-controlled data is exported to certain export-prohibited countries). It is against this backdrop that the clarifications in FAQs 25 and 26 are especially significant.

1 The CUI registry describes "export controlled" information as:
Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.

FAQs 25 and 26 generally address the interrelationship of export-controlled technical data and technology with CDI. FAQ 25 provides that export controlled information is considered CDI when it is either (1) marked as such and provided to the contractor by or on behalf of DoD or (2) "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the [DoD] contract." FAQ 25 goes on to say that "when DoD contractors hold information that is export controlled and that is related to the DoD activity in performance of the contract, the information requires safeguarding."

DoD pronouncements prior to FAQ 25 noted that not all contractor information that was "used" by the contractor in support of the performance of a DoD contract constitutes CDI. Such information includes "information in the contractor's human resources or financial/accounting systems," which DoD apparently views as incidental to performance of a particular contract. Drawing on this example, pre-existing export controlled data residing on a contractor's information system could also reasonably be regarded as incidental to performance of a particular DoD contract. Therefore, even if the contractor used pre-existing export controlled information in support of its performance of a DoD contract, that information would not thereby become CDI. However, FAQ 25 makes no reference to any exception when it comes to export-controlled information. Rather, it states that, "[w]hen DoD contractors hold information that is export controlled and is related to the DoD activity in performance of the contract, the information requires safeguarding" — period. This stands in contrast to the language in DoD's response to FAQ 29, which notes that information in the contractor's human resources or financial/accounting is not considered CDI even if it is used by the contractor to support contract performance.

Furthermore, while FAQ 26 explains that the DFARS safeguarding clause "only applies to export controlled information that meets the definition of covered defense information," it goes on to state that the -7012 Clause "requires the contractor to provide adequate security on the information *systems* that process, store, or transmit covered defense information" (emphasis added). Thus, although the -7012 Clause "does not assign any specific safeguarding requirements to the [export controlled] information itself," the practical implication is an extension of the -7012 Clause to information systems that may not otherwise be involved in the performance of the DoD contract or safeguarded in accordance with the -7012 Clause.

Granted, companies who are already compliant with the -7012 Clause on a company-wide basis (*e.g.*, on account of their frequent engagement in DoD contracts or handling of export-controlled information) or who can effectively segment and isolate CDI-classified, export-controlled information that is newly developed for a particular contract would be able to avoid or manage significant disruption from this extension of the -7012 Clause. More commonly, however, export-controlled information predates its use in the performance of a DoD contract and may exist on information systems that are wholly unrelated to DoD contract performance. For example, export-controlled data might be shared pursuant to a manufacturing license agreement unrelated to a DoD contract and then later classified as CDI based on its use in a subsequent DoD contract in the United States. Such use could arguably trigger the -7012 Clause safeguard requirements for the data and for the entire system on which it resides.[2]

2 This would ***not*** be the case if the pre-existing export-controlled data pertained to a "commercial item." *See* Response to FAQ 2. Pursuant to the Response to FAQ 2, only documents or data describing a substantive change to the commercial item or its use or integration within DoD or a DoD system or platform require protection as CDI, "not the standard commercial item itself or associated data."

In many cases, implementation of the -7012 Clause safeguards will overlap with controls and preparations undertaken in the context of technology control plans developed pursuant to, *e.g.*, 22 C.F.R. § 126.13(c). Moreover, companies employing EAR-compliant cloud services will also be familiar with various NIST encryption and access control standards involved in the deployment of those services. *See* 15 C.F.R. § 734.18(a)(5)(iii). That said, the substantial breadth of the -7012 Clause and NIST SP 800-171 will inevitably involve careful scrutiny and resource allocations to ensure compliance with these more comprehensive standards.

More importantly, the -7012 Clause also imposes cyber incident reporting requirements that are more stringent than those imposed by export control regulations. BIS, for example, has specifically noted that data breach victims do not engage in illicit exports simply because they experience a breach. *See* 81 Fed. Reg. 35,568, 35,592 (June 3, 2016) ("This provision [*i.e.*, 15 C.F.R. § 734.15, defining "Release"] codifies the basic concept that the unwitting victim of, for example, a database hack is not the one responsible for the theft of technology."). And, notwithstanding the mandatory reporting required under ITAR's Section 121.1(e)(1), absent evidence of exfiltration or release of controlled information, neither ITAR nor EAR imposes general obligations to report mere network breaches. By contrast, the -7012 Clause requires reporting of a far broader range of cyber incidents, *i.e.*, any "compromise or an actual or potentially adverse effect on an information system and/or the information residing therein" within 72 hours after its discovery.

Against that backdrop, the extension of the -7012 Clause to systems on account of their contact with export-controlled information that has been identified as CDI could generate significant technical and compliance challenges for companies operating in the export controls space. As a technical matter, adequate safeguarding, specifically intrusion detection and breach reporting, implicates a wider array of technical capabilities and resources compared to access controls and encryption implementations involved in technology control plans—a distinction that will warrant, among other considerations, close attention to the scope of services contracts with information security vendors. On the compliance front, network penetration reporting requirements will inevitably increase the pressure on companies reporting breaches to the DoD to consider concurrent voluntary disclosures to DDTC and BIS.

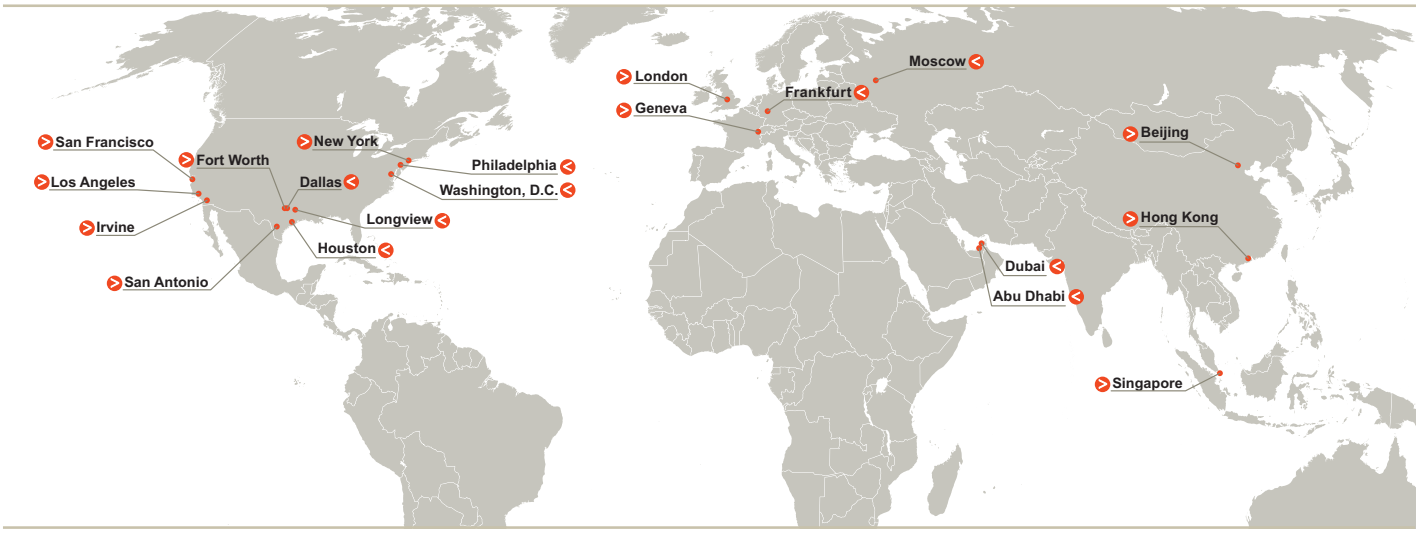
In addition to these internal considerations, the application of -7012 to pre-existing information used in DoD contracts also implicates contractual relationships with foreign recipients (future and past) of export controlled information, such as in the context of technical assistance or manufacturing license agreements authorized by DDTC. Companies that have provided, or intend to provide, export controlled information that has been or will be used in a DoD contract (particularly where the foreign recipient is not involved in the DoD contract) must take care to draft and enforce contractual obligations that provide for compliance with -7012 and NIST SP 800-171—an effort complicated by DOD's ongoing negotiations with countries whose laws prohibit the types of reporting required by -7012. *See* Response to FAQ 9.

4. Conclusion

The enactment of the -7012 Clause and related draft DoD guidance are just the latest steps with regard to a continuing cycle of cybersecurity framework developments. This DFARS provision and the guidance both provide clarification for contractors with regard to their responsibilities and raise the specter of increased regulatory burdens beyond those already mandated under existing frameworks (*e.g.*, ISO 27001, FedRAMP). What is clear is that DoD's approach to implementing these provisions and its overall cybersecurity framework will continue to evolve in the coming months and years.

Covered contractors will have to balance keeping up with DoD's efforts in this area with their efforts to comply with additional frameworks currently under development, both at home and abroad. In the European Union (EU), in particular, contractors will have to contend with a complex web of cybersecurity and privacy regulations, some of which are in harmony with the DFARS, while others go far beyond DoD's actions to this point. The EU's General Data Protection Regulation (GDPR) and Cybersecurity Directive are both taking effect this year and are poised to become the gold standard in privacy and cybersecurity measures. Flashpoints between DoD and GDPR provisions are bound to arise. For example, given the broad categories of information that constitute CDI and CUI under the -7012 Clause, the GDPR's mandates related to data access, rectification, deletion and modification may clash with existing ITAR and EAR compliance regimes. Developments in the EU will also require a more careful analysis of contractor and subcontractor data retention and processing policies and procedures.

These developments are just the beginning. Covered defense contractors, particularly those who fall within the terms of EU regulations, will have to increasingly parse and balance intersecting, sometimes contradictory, frameworks related to cybersecurity and privacy. What is more, it likely will not be long before the government imposes requirements similar to the -7012 Clause on all federal government contractors through the Federal Acquisition Regulation. We will further explore some of these themes in our upcoming post examining new EU regulations from the perspective of U.S. covered defense contractors.



For more information, please contact:

Robert K. Huffman
Partner
☎ +1 202.887.4530
@ rhuffman@akingump.com

Natasha G. Kohne
Partner
☎ +1 415.765.9505
@ nkohne@akingump.com

Thomas J. McCarthy
Partner
☎ +1 202.887.4047
@ tmccarthy@akingump.com

Kevin J. Wolf
Partner
☎ +1 202.887.4051
@ kwolf@akingump.com

Maureen C. McDonald
Associate
☎ +1 202.887.4537
@ maureen.mcdonald@akingump.com

Joseph W. Whitehead
Senior Counsel
☎ +1 202.887.4477
@ jwhitehead@akingump.com

Chris Chamberlain
Associate
☎ +1 202.887.4308
@ cchamberlain@akingump.com

Akin Gump

STRAUSS HAUER & FELD LLP

ABU DHABI
BEIJING
DALLAS
DUBAI
FORT WORTH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
IRVINE
LONDON
LONGVIEW
LOS ANGELES
MOSCOW
NEW YORK
PHILADELPHIA
SAN ANTONIO
SAN FRANCISCO
SINGAPORE
WASHINGTON, D.C.

Akin Gump Strauss Hauer & Feld LLP is a leading global law firm providing innovative legal services and business solutions to individuals and institutions. Founded in 1945 by Richard Gump and Robert Strauss with the guiding vision that commitment, excellence and integrity would drive its success, the firm focuses on building lasting and mutually beneficial relationships with its clients. Our firm's clients range from individuals to corporations and nations. We offer clients a broad-spectrum approach, with over 85 practices that range from traditional strengths such as appellate, corporate and public policy to 21st century concentrations such as climate change, intellectual property litigation and national security.