ADG Insights

Cybersecurity and supply-chain developments and trends for companies that conduct business with the U.S. government

April 2019

Hogan Lovells

Introduction

While all companies should be concerned with their cybersecurity posture, companies in the aerospace, defense, and government services (ADG) industry may be subject to greater risks because the industry is an attractive target for the intelligence and military arms of foreign governments, political actors of all sorts, and criminal enterprises. Continued reports of cyber compromise and new concerns about supply-chain security have caused the federal government to adopt numerous changes to cybersecurity rules and contractual requirements, which have rapidly increased the security demands on government contractors. Neither the government nor the private sector can protect systems and networks without extensive and close cooperation. Contractor noncompliance with applicable security requirements, or misrepresentations regarding a contractor's security posture, may result in government investigations, significant financial liability, and reputational harm. Therefore, it is critically important that ADG companies stay abreast of the latest safeguarding standards, contractual and regulatory requirements, and best cybersecurity practices.

I. Securing the federal supply chain

Over the past year, Congress has taken legislative action to explicitly prohibit federal government agencies from using or procuring certain covered items, to strengthen preexisting authorities for certain agencies to exclude risky sources of supply, and to provide new mechanisms the federal government can employ to identify supply-chain threats through risk-based assessments and, if necessary, ban those sources from the federal supply chain. ADG companies must scrutinize their supply chains for compliance with these new requirements in order to remain qualified to compete for certain types of contracts.

a) Congressional bans on sources of supply

- **Kaspersky Lab:** Sec. 1634 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018 (Pub. L. 115-91) prohibits agencies from directly or indirectly using any hardware, software, or services developed or provided in whole, or in part, by Kaspersky Lab.[1] The prohibition is broad and includes successor entities to Kaspersky Lab, any entity that it controls, is controlled by, or is under common control with Kaspersky Lab, or any entity in which Kaspersky Lab owns a majority share. This statutory Kaspersky Lab ban was implemented via Federal Acquisition Regulation (FAR) contract clause 52.204-23 *Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities*.[2] The clause is mandatory in all solicitations and contracts, and flows down to all subcontracts (including subcontracts for the acquisition of commercial items).
- **Telecommunications equipment or services connected to Chinese and/or Russian governments:** Sec. 1656 of the FY 2018 NDAA[3] requires the Secretary of Defense (SECDEF) to certify to Congress whether "covered telecommunications equipment or services" are used as substantial or essential components of any system, or as critical technology as part of any system, that is used to carry out nuclear deterrence or homeland defense.[4] Beginning one year after the enactment of the NDAA, the section further prohibits the U.S. Department of Defense (DoD) from procuring or obtaining any equipment, system, or service that relies on such covered items to carry out the nuclear deterrence or homeland defense missions. An open Defense Federal Acquisition Regulation Supplement (DFARS) case, 2018-D022, *Covered Telecommunications Equipment or Services,* will implement Sec. 1656 for DoD procurements.

  Sec. 889 of the FY 2019 NDAA (Pub. L. 115-232)[5] considerably expands on the prohibition contained in section 1656 of the FY 2018 NDAA with respect to purchasing or obtaining any equipment, system, or service that relies on "covered" items. Section 889 expands upon the definition of covered items in Section 1656 by not being limited to systems for the nuclear deterrence or homeland defense missions; instead, it applies to all federal agencies (not just DoD) and to all missions. It covers loans and grants as well as procurements of surveillance services and equipment and telecommunications equipment and services. It also prohibits (effective August 13, 2020) entering into a contract or extending a contract with an entity that uses any covered equipment or services as a substantial or essential component of any system. An open FAR Case, 2018-017, *Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment,* will implement Sec. 889 for all federal agencies.

b) Strengthened federal exclusion authorities

Under Sec. 881 of the FY 2019 NDAA, the SECDEF (and the Secretaries of the Army, Navy, and Air Force), may exclude certain sources of supply in order to reduce supply-chain risk and limit the disclosure of information relating to the basis for any such exclusion.[7] This authority has existed since 2011 but, according to public DoD statements, has never been utilized. The FY 2019 NDAA repealed a sunset provision that would have caused the prior authority to expire on September 30, 2018 and made this authority permanent.[8] It remains to be seen if, now that this "Section 881 authority" is permanent, DoD will start using this exclusionary authority more.[9]

This authority may only be exercised after several steps have been taken related to the proposed exclusion, including the following:

- A joint recommendation must be obtained from the Under Secretary of Defense for Acquisition and Sustainment and the DoD's chief information officer that supports the planned exclusion based on a risk assessment by the Under Secretary of Defense for Intelligence.
- There must be a finding that the action is necessary and there are no other less intrusive options available.
- In a case where disclosure of the basis for the action is to be withheld, the Secretary concerned must find the risk to national security of the disclosure outweighs the risks associated with not disclosing the information. Of note, when this particular authority to limit disclosure is exercised, the exclusion of the source is not reviewable in a bid protest before the U.S. Government Accountability Office (GAO) or in federal court.
- Finally, notice must be given to the appropriate congressional committees.

Another recently adopted statutory provision, FY 2019 NDAA Sec. 3117, extends U.S. Department of Energy (DOE) authority to manage supply-chain risk to June 30, 2023.[10] The DOE Secretary's authority, detailed at 50 U.S.C. 2786, is substantially similar to the now permanent Section 881 authority for DoD and allows the Secretary to exclude sources and withhold consent to subcontract for covered systems and components (e.g., national security systems, nuclear weapons, certain surveillance systems, and nonproliferation programs and systems).

In addition to the above provisions that enable government agencies to exclude certain sources of supply in order to reduce supply-chain risk, Section 1655 of the FY 2019 NDAA,[11] qualifies DoD's ability to use other suppliers on certain disclosures. Specifically, DoD "may not use a product, service, or system procured or acquired … relating to information or operational technology, cybersecurity, an industrial control system, or weapons system," unless certain information is disclosed to DoD, including:

- Whether a foreign person and/or government has been allowed or will be allowed to review the code of noncommercial products, services, or systems developed for DoD within five years prior to the enactment of the NDAA or anytime thereafter.
- Whether an organization or person has allowed within the five years prior to the enactment of the NDAA, or is under an obligation to allow, a foreign government or person from the countries listed in Section 1654, *Identification of Countries of Concern Regarding Cybersecurity,* to review the source code of a product, system, or service that DoD is using or intends to use.[12]
- Whether export licenses have been held or sought for the export of information technology (IT) products, components, software, or services that contain code developed for or used by DoD.

The SECDEF is directed to issue regulations implementing these supply-chain disclosure requirements. Furthermore, within a year, a registry must be created to collect and maintain information disclosed and made available to any federal agency conducting a FAR-based procurement.

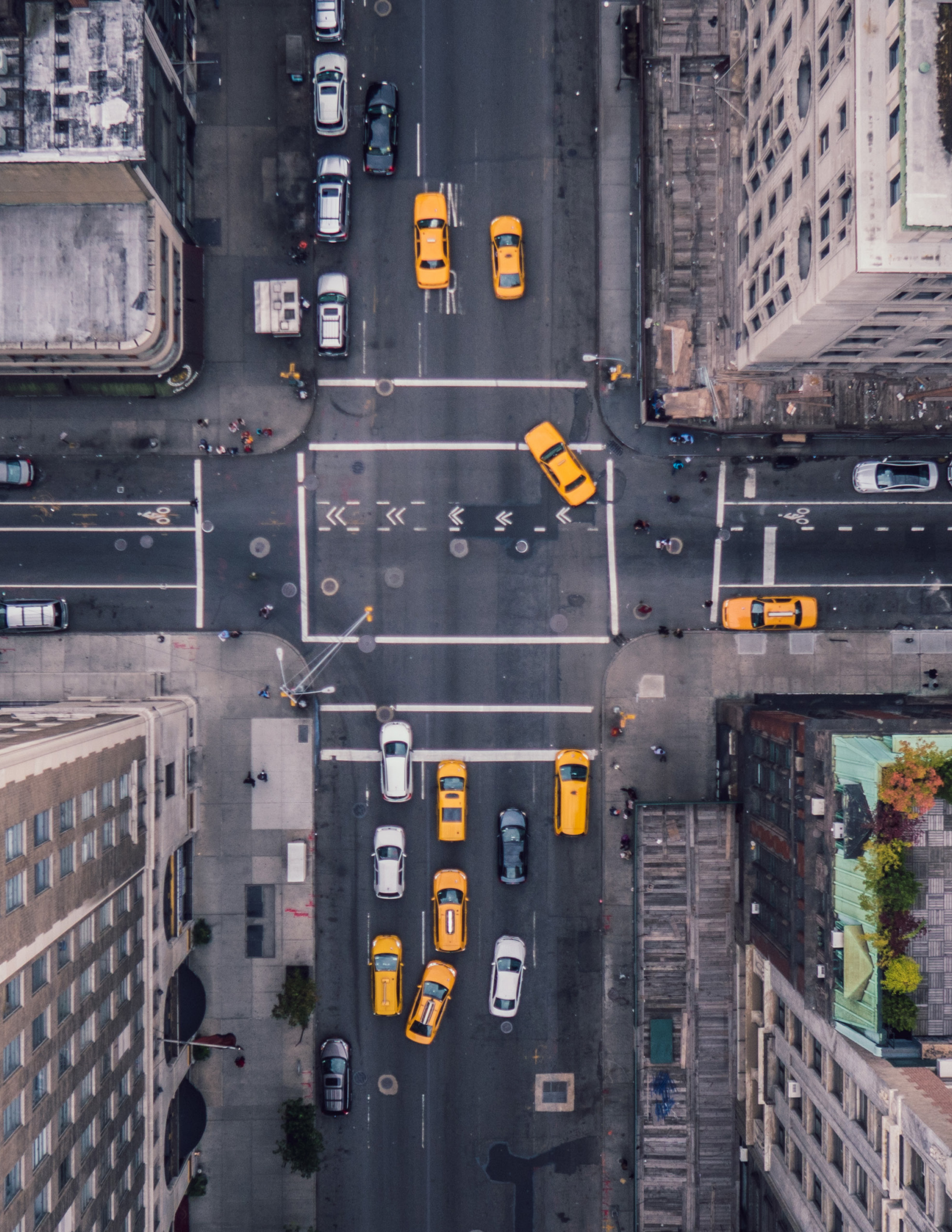
Upon receipt of disclosures, the SECDEF will evaluate any risks to national security – if the SECDEF determines such disclosures reveal "a risk to the national security infrastructure or data of the United States, or any national security system under the control of the Department," the SECDEF shall take appropriate mitigation actions, including "conditioning any agreement for the use, procurement, or acquisition of the product, system, or service on the inclusion of enforceable conditions or requirements that would mitigate such risks." Additionally, within two years of the enactment of the 2019 NDAA, DoD must develop testing standards for commercial off-the-shelf products "to use when dealing with foreign governments."

c) IT exclusion and removal criteria under development

On December 21, 2018, President Trump signed into law the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act) (Pub. L. 115-390). Among other features, the act incorporates in Title II the "Federal Acquisition Supply Chain Security act of 2018," which creates a new Federal Acquisition Security Council whose functions include:

- Making recommendations to the National Institute of Standards and Technology (NIST) regarding the development of supply chain risk management (SCRM) standards.[13]
- Creating procedures for information sharing.
- Setting criteria and procedures that can be used to exclude certain sources of supply in IT acquisitions.

The law requires federal agencies to assess security risks in their supply chains when purchasing IT products and authorizes the government to mitigate such threats by using "exclusion and removal" orders, for which the new council will establish the criteria and procedures. These orders would either require the exclusion of covered items from the agency procurement action or require the removal of the covered items from federal agency information systems.[14] The council must identify exceptions to the criteria for exclusion and removal, make risk assessments of the covered items, provide a summary of the basis of the order, and identify how a source may mitigate the risk to get an order rescinded. A source must be notified of a recommendation for exclusion or removal, the criteria used, and the basis for the recommendation "to the extent consistent with national security and law enforcement interests."[15] Judicial review is available exclusively through the D.C. Circuit Court of Appeals and a petition for judicial review must be filed within 60 days after notification of the order – analogous to DoD's Section 806 (now 881) authority discussed above, a contractor cannot submit a bid protest about such exclusion to the GAO.



II. Enhanced requirements and standards for ADG entities that handle government information

On September 14, 2016, the National Archives and Records Administration (NARA) released its long-awaited Controlled Unclassified Information (CUI) Final Rule (CUI regulation),[16] which prescribes the requirements governing agency safeguarding, marking, and disposal of CUI. The CUI regulation, codified at 32 Code of Federal Regulations Part 2002, established the CUI Registry as the official online repository for information, guidance, policy, and requirements for federal agencies to follow in handling CUI, and prescribes the use of NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,* when CUI will reside on nonfederal (i.e., contractor) information systems.

Although the CUI Final Rule was published over two years ago, DoD is the only agency that has specifically addressed CUI safeguarding by its contractors –through contract clauses detailed in DFARS provisions and discussed further below –in accordance with the CUI regulation. However, although the government is still developing a FAR case for governmentwide implementation,[17] the CUI regulation already directs agencies to "include provisions that [*require the non-executive branch entity to*] handle the CUI in accordance with the Order, this part, and the CUI Registry" in any written agreements with nonexecutive branch agencies (including contracts, grants, licenses, certificates, and other agreements) that involve CUI. Therefore, until the standard FAR provision is effective, contractors with different agency customers could find themselves subject to potentially conflicting and duplicative agency-specific agreement provisions regarding CUI.[18] It is imperative that contractors identify and understand the terms and conditions in their contracts and take measures to ensure compliance.

The NIST standards themselves have continued to undergo changes over the past year:

- On June 7, 2018, NIST issued an erratum update of NIST SP 800-171 with new references and definitions, an Appendix F section on "discussion" of each CUI requirement, and minor editorial changes to the 110 security requirements themselves. NIST has also publicly announced that a complete "Revision 2" to 800-171 will be released in 2019.
- On June 13, 2018, NIST released the final version of SP 800-171A *Assessing Security Requirements for Controlled Unclassified Information*. This publication serves as a companion piece to SP 800-171 by providing both federal and nonfederal entities with "assessment procedures and a methodology" to help "conduct efficient, effective, and cost-effective assessments" of the CUI security requirements in SP 800-171.
- On October 18, 2018, NIST announced at a CUI Security Requirements Workshop in Gaithersburg, Maryland, that it planned to add "enhanced CUI security requirements" in the next revision of SP 800-171, with the intent to address "advanced persistent threats" (APT) and to prevent the theft or compromise of highly sensitive federal information." More recently, NIST officials have publicly stated that these additional requirements will now appear in a separate, companion publication, NIST 800-171B *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for High Value Assets,* with the intent that federal agencies can use these additional protection measures on a case-by-case basis when CUI is part of a critical program or high-value asset.

Accordingly, ADG companies, when serving as government contractors, are facing an increasing number of cybersecurity requirements. Companies that do not have adequate safeguards in place risk termination, financial liability, reputational harm, and are disadvantaged competitively when competing against contractors that have implemented the necessary safeguards.

III. Increased DoD scrutiny on ADG entities cybersecurity posture and oversight of subcontractors

As of this writing, DoD is still the only agency mandating in its acquisition regulations that its covered contractors meet the requirements in the CUI regulation for safeguarding CUI on contractor systems. The DoD "safeguarding" clause, DFARS 252.204-7012, requires "adequate security" on "covered systems," which includes meeting, at a minimum, all of the 800-171 requirements. This year, although DoD refrained from making any more changes to the DFARS contract clauses themselves, various DoD guidance documents were issued addressing how DoD contracting entities should implement the DFARS requirements. Although these guidance documents were directed to DoD contracting and acquisition personnel, they will ultimately affect contractors.

The mandates embedded in these recent guidance documents (in particular the most recent one from February) demonstrate that DoD continues to prioritize cybersecurity compliance and the flow-downs are becoming a critical part of DoD's overall plan to guard against cyber incidents. It is becoming imperative for DoD prime contractors to review their security policies and procedures when it comes to DoD CUI and to ensure that, at a minimum, their first-tier subcontractors also have a robust understanding of the DoD cybersecurity requirements and adequate procedures to safeguard such information.

Recent DoD guidance related to CUI include:

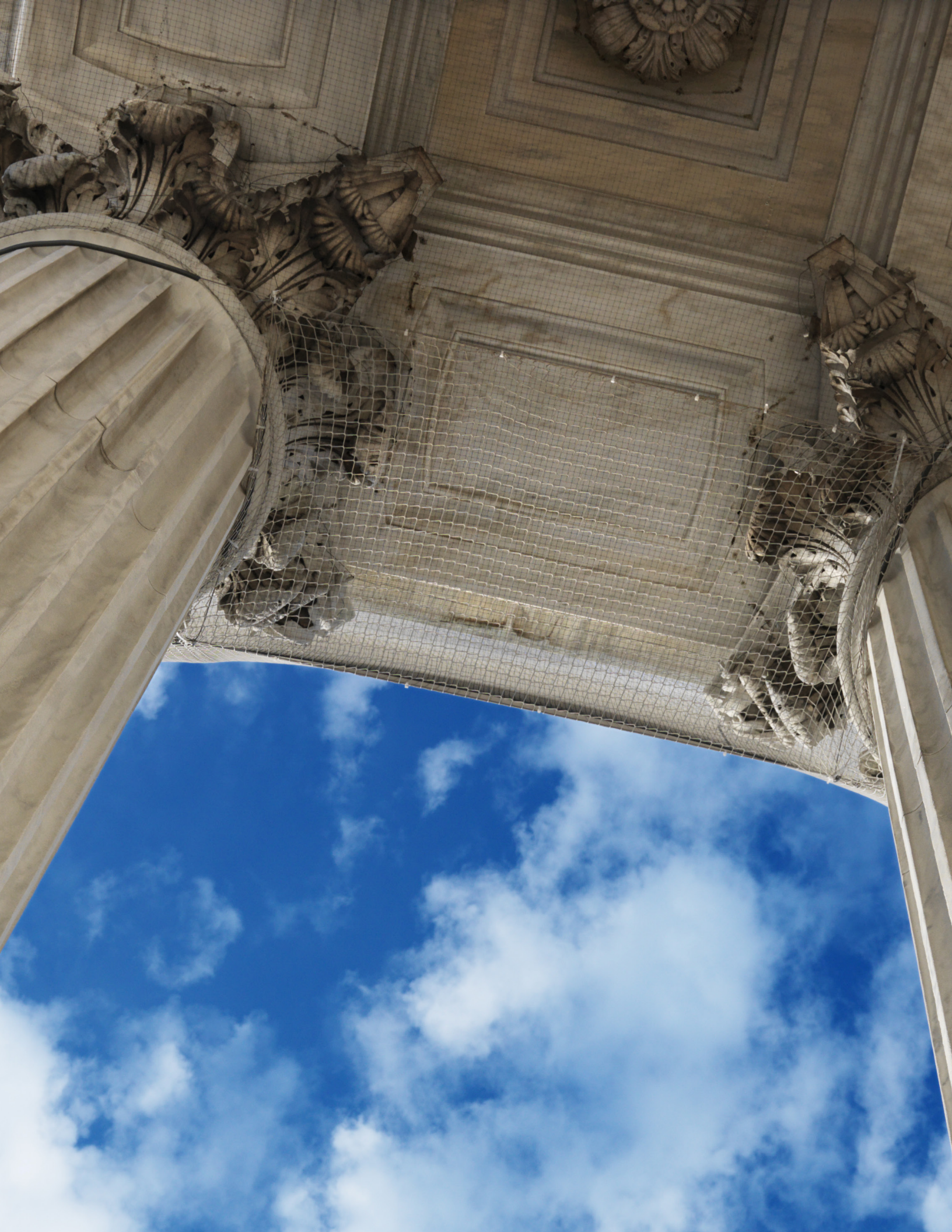
- DoD Defense Pricing and Contracting (DPC) *Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012* (November 6, 2018): In November 2018, the DPC office issued guidance[19] to acquisition personnel on assessing a contractor's approach to providing adequate security required by the DFARS 7012 clause in both pre-award and post-award scenarios. The DPC guidance provides a framework that can be tailored by the DoD customer, commensurate with program risk, to assess a contractor's approach to protecting DoD CUI. A companion document, *DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Requirements Not Yet Implemented,* is intended to provide for consistent review of system security plans (SSPs) and plans of action and milestones (POA&Ms) when such plans are required by the solicitation or contract to be provided to the government (e.g., in a Contract Data Requirements List (CRDL)). The guidance is intended to help the DoD customer determine the impact of 800-171 security requirements "not yet met" by the contractor.
- Assistant Secretary of the Navy for Research, Development & Acquisition (ASN RDA) memorandum, *Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks* (September 28, 2018): News stories indicate that the U.S. Navy suffered a significant cyber breach in 2018 when an attacker reportedly hacked a Navy contractor and exfiltrated sensitive information on submarine warfare. Subsequently, the ASN RDA issued a memorandum on September 28, 2018, directing that the Navy take "immediate steps to increase the protection of its critical information." When a program manager determines "risk to a critical program and/or technology," the memorandum requires that a CDRL include delivery and approval of the contractor's SSP that implements the security requirements of the DFARS 7012 clause. The CDRL must also permit the government to validate the contractor's information contained in the SSP every three years, on an ad hoc basis with no notice to the contractor, or upon replacement or rotation of the government program manager. In addition, program managers are to require the contractor to allow the Naval Criminal Investigative Service (NCIS) to install network sensors when intelligence indicates a potential, or actual, vulnerability.
- Assistant Secretary of Defense for Acquisition (ASD(A)) memorandum, *Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base* (December 17, 2018): This memorandum includes sample statement of work (SOW) language addressing DoD access to/delivery of a contractor's SSP that can be used by DoD customers in conjunction with the sample CDRL language included in the DPC guidance from November. This memorandum also includes sample language to track a contractor's flow-down of DoD CUI requirements to its tier 1 subcontractors/suppliers.
- Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) memorandum, *Addressing Cybersecurity Oversight as part of a Contractor's Purchasing System Review* (January 21, 2019): In this memorandum, the OUSD(A&S) directs the Defense Contract Management Agency (DCMA) to audit and evaluate how prime contractors are assessing how their tier 1 subcontractors/suppliers are complying with the DoD cybersecurity requirements when subcontract performance will involve DoD's CUI.
- OUSD(A&S) memorandum, *Strategically Implementing Cybersecurity Contract Clauses* (February 5, 2019): This latest memorandum from OUSD(A&S) states that the individual contract approach to DFARS 7012 is "inefficient for both industry and government, and impedes the effective implementation of requirements to protect DoD's Controlled Unclassified Information…". Therefore, the memorandum directs the DCMA to develop a proposed strategy to use its authority to modify contracts, as a no-cost bilateral block change, to accomplish the following:
  - Require the delivery of a contractor's SSP (or extracts thereof), and any associated POA&Ms, at the strategic level.
  - Document industry cybersecurity readiness at a strategic level.
  - Apply a standard methodology to recognize cybersecurity readiness at a strategic level.

The road ahead

ADG companies should anticipate the increased cybersecurity and supply-chain integrity concerns to continue to impact how they do business with the federal government. Specifically, companies should prepare for the following:

Increased DoD scrutiny of contractor cybersecurity posture

- Based on the various memoranda from DoD, DCMA audits of contractor cybersecurity are forthcoming. Separately, the DoD Office of Inspector General (IG) announced in June 2018 that it was initiating cybersecurity audits that would include select contractors.
- Contractors should expect to see cybersecurity as a source-selection criteria (i.e., the DPC guidance documents strongly recommend DoD customers use cyber as a criteria).
- Contractors should be prepared to actually provide their SSPs and POA&Ms (or extracts thereof) for DoD review. Previously, the DoD cybersecurity requirement relied on "self-attestation" by contractors (i.e., do you or do you not have an SSP and POA&M in place). Now, based on the successive guidance materials within DoD, it is increasingly likely that DoD ordering activities will require delivery of/access to SSPs and POA&Ms.

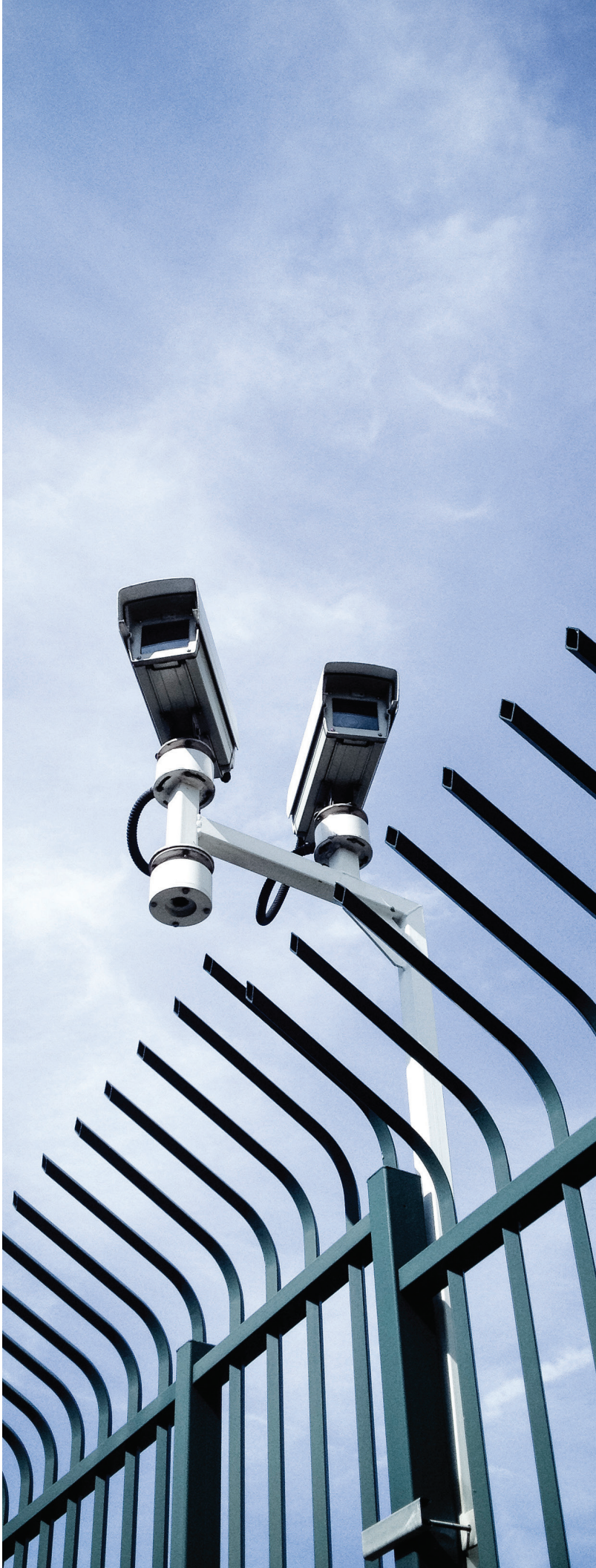


Potential security controls above and beyond the DFARS 7012 clause & NIST 800-171 baseline

- For example, the ASN RDA memorandum explicitly requires enhanced security controls and the possibility of NCIS installing sensors on the contractor's network when intelligence indicates a vulnerability or potential vulnerability. Furthermore, the forthcoming NIST 800-171B document will introduce a whole new set of potential security requirements for high-risk programs. Note that the DFARS 7012 clause has always allowed for additional security requirements above and beyond 800-171 – but now it may become a standard practice with DoD customers.

Increased pressure on primes to manage their supply chains

- The DCMA has been directed to review whether primes flow down DoD CUI requirements to suppliers when the subcontract will involve DoD's CUI. The DoD guidance documents above also include sample SOW and CDRL language that contemplate requiring primes to identify when they actually provide CUI to their subcontractors.
- The ultimate message from all of these DoD guidance documents is that prime contractors and, at a minimum, their first-tier subcontractors, must take all appropriate steps to safeguard DoD information, that the cybersecurity flow-downs are material contract requirements, and that DoD is going to view noncompliance unfavorably.
- In short, supply-chain security is rapidly moving from a theoretical concern to front and center in the acquisition process. Companies up and down the supply chain must be prepared to demonstrate that they have effective security controls in place and that they are implementing those controls. Having good security plans on the shelf will not be enough as we move through 2019 into 2020.



Authors and contacts

Michael J. Scheimer
Senior Associate, Washington, D.C.
T +1 202 637 6584
michael.scheimer@hoganlovells.com

Michael F. Mason
Partner, Washington, D.C.
T +1 202 637 5499
mike.mason@hoganlovells.com

Robert Taylor
Senior Counsel, Washington, D.C.
T +1 202 637 5657
bob.taylor@hoganlovells.com

Stacy Hadeka
Senior Associate, Washington, D.C.
T +1 202 637 3678
stacy.hadeka@hoganlovells.com

Rebecca Umhofer
Knowledge Lawyer, Washington, D.C.
T +1 202 637 6939
rebecca.umhofer@hoganlovells.com

Endnotes

1. Sec. 1634. *Prohibition on use of products and services developed or provided by Kaspersky Lab*.
2. On June 15, 2018, the FAR Council issued this as an interim rule effective July 16, 2018. 83 Fed. Reg. 28,141 (June 15, 2018). This rule-making follows the Department of Homeland Security's September 2017 directive instructing all agencies to identify and purge Kaspersky products from their systems, *Binding Operational Directive 17-01*, 82 Fed. Reg. 43,782 (Sept. 19, 2017).
3. Sec. 1656. *Security of nuclear command, control, and communications system from commercial dependencies*.
4. Covered telecommunications equipment or services is defined as telecommunications equipment produced by Huawei Technologies Company (Huawei) or ZTE Corp. (ZTE) (or any subsidiary or affiliate of such entities); telecommunications services provided by such entities or using such equipment; or telecommunications equipment or services produced or provided by any other entity that the SECDEF (in consultation with the Federal Bureau of Investigation (FBI) and Director of National Intelligence (DNI)) reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country (defined in this section as China or Russia).
5. Sec. 889. *Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment*.
6. In one respect the prohibition in Section 889 is narrower – a "covered" foreign country is defined in Section 889 as being China and only China (Russia is not included).
7. Sec. 881. *Permanent Supply Chain Risk Management Authority* (codified at 10 U.S.C. §2339a)
8. The original authority under Section 806 of the FY 2011 NDAA is for procurements relating to particular types of systems (national security systems) that include, but are not limited to, classified information systems.
9. DoD issued a final rule implementing this section on February 15, 2019, removing the sunset date and correcting various statutory references, but making no substantive changes to the DFARS rule that had implemented section 806 of the NDAA for FY 2011. 84 Fed. Reg. 4368, DFARS Case 2018–D072 (Feb. 15, 2019).
10. Sec. 3117. *Extension of enhanced procurement authority to manage supply chain risk*.
11. This provision is subject to forthcoming regulations (i.e., DFARS case 2018-D064 Disclosure of Information Regarding Foreign Obligations).
12. Sec. 1654. I*dentification of Countries of Concern Regarding Cybersecurity,* directs the SECDEF to "create a list of countries that pose a risk to the cybersecurity of United States defense and national security systems and infrastructure. Such list shall reflect the level of threat posed by each country included on such list."
13. DoD has indicated that it will leverage the Federal Acquisition Security Council to assist in creating a uniform cybersecurity standard for all executive agencies. Contractors should expect to see this addressed through a standard notice and comment period.
14. Interestingly, given the geographic focus of the bans in the 2018 and 2019 NDAAs, the final amended version of the SECURE Technology Act that passed the Senate says specifically that the government may not simply ban products or companies via exclusion or removal orders "based solely on the fact of foreign ownership of a potential procurement source" if otherwise qualified to contract with the federal government.

    Section 1323 "(f) Rules Of Construction.—Nothing in this section shall be construed—

    > *"(1) to limit the authority of the Office of Federal Procurement Policy to carry out the responsibilities of that Office under any other provision of law; or*
    >
    > *"(2) to authorize the issuance of an exclusion or removal order based solely on the fact of foreign ownership of*
    >
    > *a potential procurement source that is otherwise qualified to enter into procurement contracts with the Federal Government*

15. Classified and otherwise privileged information, such as law enforcement information, that formed the basis for the exclusion is to be submitted to the court ex parte and is not to be shared with the petitioner.
16. 81 Fed. Reg. 63,324 (Sept. 14, 2016).
17. FAR case No. 2017-016 Controlled Unclassified Information.
18. 32 C.F.R. §2002.16(a).
19. *Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System*.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Associated offices

www.hoganlovells.com