THE NASH & CIBINIC REPORT
government contract analysis and advice monthly from professors ralph c. nash and john cibinic

Author: Ralph C. Nash, Professor Emeritus of Law, The George Washington University
Contributing Authors: Vernon J. Edwards and Nathaniel E. Castellano

NOVEMBER 2024 | VOLUME 38 | ISSUE 11

¶ 65 INFORMATION SECURITY: Today's Top Compliance Challenge For Government Contractors

A special column by Thomas A. Pettit, Senior Associate in the Government Contracts and National Security practice group at Arnold & Porter; the ideas presented here, particularly those that may prove to be in error, are the author's own and should not be attributed to any other.

Information security is a relatively broad concept that encompasses safeguarding and handling regulated and other sensitive data, including confidential and proprietary business information. Government contracts often involve extensive regulated data with varying (and overlapping) levels of sensitivity, ranging from (1) simple transactional information subject to few restrictions, to (2) Controlled Unclassified Information (CUI) subject to disparate security requirements, all the way to (3) classified information that is highly restricted and, if disclosed improperly, could catastrophically harm the national security of the United States. Given the consequences of improper handling and disclosure of regulated data, Government contractors, including prime contractors and subcontractors, are typically subject to a patchwork of information security requirements, depending on the types of information they handle.

Information security requirements in Government contracts generally fall into two categories. The first category encompasses regulations that require contractors to safeguard specific types of information. The second category encompasses regulations that are not tied to particular information but rather seek to shore-up the supply chain for information technology and related services.

The use of contract terms to impose information security requirements is a relatively young area of Government contracts law, but the Government's focus on compliance and enforcement is increasing quickly. This *Guest Appearance* provides an overview of the information security regulatory landscape for Government contractors, recent developments, and takeaways for current and prospective Government contractors. These requirements are evolving quickly, and there are several ongoing rulemakings that could expand Government contractors' compliance obligations.

Information-Specific Requirements

Government contractors that receive or produce sensitive information during contract performance encounter increasingly complex information security requirements. Those obligations vary by agency and the nature of the information. Below are some of the most significant Federal Acquisition Regulation, Defense FAR Supplement, and Homeland Security Acquisition Regulation provisions in this category.

• *FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems*"— This clause establishes some of the most basic requirements for contractors with information systems that store, process, or transmit federal contract information (FCI), which is among the least sensitive types of information for Government contracts. FAR 52.204-21 defines FCI broadly as "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government" but excludes information the Government made publicly available and "simple transactional information, such as [information] necessary to process payments." FAR 52.204-21(a). The clause directs contractors with covered information systems to meet 15 requirements. Some of those requirements are subject to interpretation, but they encompass relatively basic security measures, including limiting access to covered information systems, maintaining antivirus and similar software to protect against malicious code, periodically scanning information systems for malicious code, and implementing facility security measures (e.g., "[e]scort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices"). FAR 52.204-21(b)(1).

• *DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting*"—This clause imposes more onerous information security requirements for Department of Defense contracts. First, contractors must "provide adequate security" for information systems that store, process, or transmit covered defense information (CDI). DFARS 252.204-7012(b). CDI is defined as CUI that is "(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." DFARS 252.204-7012(a).

What constitutes "adequate security" under the DFARS 252.204-7012 clause depends on the nature of the information system. Non-federal covered contractor information systems must comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, and third-party cloud services must "meet[] security requirements equivalent to" the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline. DFARS 252.204-7012(b)(2). On December 21, 2023, the DOD issued a memorandum detailing what it means for cloud services to be FedRAMP Moderate equivalent. DOD, *Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings* (Dec. 21, 2023), https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf. Cloud services "operated on behalf of the Government" must comply with DFARS 252.239-7010, *Cloud Computing Services*, and other information technology services and systems operated on behalf of the Government must comply with other requirements identified in the contract, such as NIST SP 800-53 and authorization to operate requirements. DFARS 252.204-7012(b)(1).

The DOD is nearing the end of its years-long process of establishing the Cybersecurity Maturity Model Certification (CMMC) program. On October 15, 2024, the DOD issued a final rule creating the CMMC program and is working to finish the rulemaking process that will amend the DFARS to apply CMMC requirements to defense contractors. CMMC will overhaul requirements for covered contractor information systems, including creating self-assessment and third-party certification requirements for applicable security controls depending on the CMMC level and contract requirements. 89 Fed. Reg. 83092.

Second, contractors must "rapidly" report cyber incidents within 72 hours of discovery. DFARS 252.204-7012(c). Relatedly, contractors must submit malicious software to the DOD Cyber Crime Center, "preserve and protect images of all known affected information systems…and all relevant monitoring/packet capture data for at least 90 days" after submitting a cyber incident report, and cooperate with DOD damage assessments and forensic analyses. DFARS 252.204-7012(c)–(g).

● *DFARS 252.204-7019, "Notice of NIST SP 800-171 DoD Assessment Requirements," and DFARS 252.204-7020, "NIST SP 800-171 DoD Assessment Requirements*"—DFARS 252.204-7019 requires offerors subject to DFARS 252.204-7012 to undergo a NIST SP 800-171 assessment in accordance with DFARS 252.204-7020 and have a current assessment score (i.e., a score from an assessment conducted within the past three years) in the DOD Supplier Performance Risk System (SPRS) to be eligible for award of a prime contract. DFARS 252.204-7020 also prohibits prime contractors from awarding a subcontract if the prospective subcontractor has not completed the required assessment. DFARS 252.204-7020(g)(2) ("The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.").

The NIST SP 800-171 DoD Assessment must, at a minimum, meet the requirements for a Basic Assessment that "[i]s based on the Contractor's review of their system security plan(s) associated with covered contractor information systems," as defined in DFARS 252.204-7012; must be "conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology"; and "[r]esults in a confidence level of 'Low' in the resulting score, because it is a self-generated score." DFARS 252.204-7020(a). Medium and High assessments are Government compliance assessments at varying levels of depth and are typically performed by the Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center. The new CMMC program could obviate some of these requirements.

● *HSAR 3052.204-72, "Safeguarding of Controlled Unclassified information*"—Similar to DFARS 252.204-7012, HSAR 3052.204-72 requires contractors to provide adequate security to protect CUI and other forms of sensitive information in accordance with a variety of DHS policies. That clause also imposes cyber incident reporting requirements, though the timelines are much shorter and range from one hour to eight hours depending on the information involved. Given the cyber threats adversaries pose to critical infrastructure and other resources, DHS has also begun imposing cybersecurity requirements in certain industries, including those related to transportation and energy. See Transportation Security Administration Press Release, *TSA Issues New Cybersecurity Requirements for Airport And Aircraft Operators* (Mar. 7, 2023), https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft; Transportation

Security Administration Press Release, *TSA Updates, Renews Cybersecurity Requirements for Pipeline Owners, Operators* (July 26, 2023), https://www.tsa.gov/news/press/releases/2023/07/26/tsa-updates-renews-cybersecurity-requirements-pipeline-owners.

• *Significant Proposed Rules*: There are a number of significant rulemakings in addition to CMMC that are in process. One such rulemaking is the proposed FAR security incident reporting rule issued in October 2023. 88 Fed. Reg. 68055 (Oct. 3, 2023). If enacted, that rule would require contractors performing contracts that use or provide Information and Communications Technology (ICT) to, among other things, report security incidents. The proposed rule defines the term security incident broadly to encompass any violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Another forthcoming proposed rule is the FAR CUI rule, which, pursuant to Executive Order 13556, "Controlled Unclassified Information," will establish FAR policies and contract clauses "for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI." FAR Case No. 2017-016, https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf.

Supply Chain-Focused Regulations

The clauses outlined above and similar types of provisions are tied to particular types of information. Other information security requirements apply regardless of the nature of information involved and are intended to mitigate supply chain risks. Below is an overview of some of these types of contract clauses that Government contractors face.

• *FAR 52.204-23, "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities*"—This clause prohibits contractors from providing the Government with, or using during contract performance, "any hardware, software, or service" or "components using any hardware or software…developed or provided by" Kaspersky Lab, any entity that owns or controls Kaspersky Lab, or any entity that Kaspersky Lab owns or controls. Contractors must timely report violations of this prohibition to the Government.

• *FAR 52.204-25, "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment" (also known as "Section 889")*—This clause, which implements § 889 of the National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, prohibits federal agencies, with certain exceptions, from purchasing and contractors from using covered telecommunications services or products from Huawei Technologies Co., ZTE Corporation, and certain other Chinese companies and their subsidiaries as an essential or substantial component of any system or as critical technology of a system. This prohibition can apply even if the contractor is not using the covered telecommunications services or products to perform a Government contract. A company that fails to comply with these requirements is ineligible to do business with the Government absent a waiver. FAR 52.204-25 requires contractors to conduct a "reasonable inquiry" that does not require internal or third-party audits. Contractors must report noncompliances within one business day of discovery and provide additional information within ten business days.

• *FAR 52.204-27, "Prohibition on a ByteDance Covered Application*"—This clause prohibits contractors "from having or using a covered application," defined as "the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited," on "information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract."

FAR 52.204-27(a)–(b). This prohibition extends to information technology "equipment provided by the Contractor's employees." FAR 52.204-27(b). TikTok is not limited solely to the downloadable TikTok application, but rather encompasses any TikTok service, including the TikTok website.

● *Federal Acquisition Supply Chain Security Act (FASCSA) Orders*—FAR 52.204-28, FAR 52.204-29, and FAR 52.204-30, which apply based on the type of contract, prohibit contractors without a waiver from providing or using to perform a contract any "any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order." FAR 52.204-30(b)(1). Covered articles include information technology, telecommunications equipment and services, processing of information on an information system subject to the CUI program, and "hardware, systems, devices, software, or services that include embedded or incidental information technology." FAR 52.204-30(a). FASCSA orders can be found in the System for Award Management (SAM), the solicitation, or a contract modification. FAR 52.204-30(b)(3)–(4). Contractors must review SAM "at least once every three months" or as the Contracting Officer directs. FAR 52.204-30(c). If a contractor discovers it provided or used a prohibited product or service, it must report the noncompliance within three business days and provide additional information within 10 business days. FAR 52.204-30(c)(4).

Compliance Risks

Contractors that do not comply with information security requirements face significant risks, including bid protests, contract disputes, and False Claims Act liability.

● *Bid Protests*—The Government Accountability Office's decision in *American Fuel Cell & Coated Fabrics Co.*, Comp. Gen. Dec. B-420551, 2022 CPD ¶ 139, 2022 WL 2116235, illustrates how noncompliance with information security requirements can render an offeror ineligible for award. The solicitation incorporated DFARS 252.204-2019 and DFARS 252.204-7020. Although the GAO denied the protest because it found the protester failed to show prejudice, the GAO held that when a solicitation incorporates DFARS 252.204-2019, an offeror is ineligible for award if it has not performed a NIST SP 800-171 Assessment in accordance with DFARS 252.204-7020. A more recent GAO decision may give prospective contractors some comfort for other information security requirements. In *Pitney Bowes, Inc.*, Comp. Gen. Dec. B-422528, 2024 CPD ¶ 123, 2024 WL 2801536, the GAO dismissed the protester's allegations that the awardee was noncompliant with DFARS 252.204-7012 and ineligible for award because, unless a solicitation requires an offeror to demonstrate compliance with that clause, those issues are matters of contract administration outside the scope of GAO's bid protest jurisdiction.

● *Contract Disputes*—If a contractor fails to comply with information security requirements, the Government could terminate the contract, including for default, or otherwise pursue damages through a Government claim under the Contract Disputes Act. *Arcade Travel, Inc. d/b/a Boersma Travel Services*, ASBCA 62009, 20-1 BCA ¶ 37,641, 2020 WL 4379241, illustrates some of these risks. In that case, the DOD terminated a contract for default and sought more than $300,000 in damages following a data breach because the contractor allegedly failed to comply with NIST SP 800-171 in violation of DFARS 252.204-7012. The contractor appealed the termination for default to the board. Although there is no public decision showing how the appeal was resolved, this case illustrates some of the Government's potential contractual remedies.

● *FCA Liability*—In October 2021, the Department of Justice announced the Civil Cyber-Fraud

Initiative. The goal of that initiative is to pursue FCA actions to "extract very hefty fines" from those "entrusted with government dollars" or "entrusted to work on sensitive government systems" who "fail to follow cybersecurity standards." Frank Konkel, *DOJ To Hit Government Contractors with "Very Hefty Fines" If They Fail To Disclose Data Breaches*, NextGov (Oct. 6, 2021), https://www.nextgov.com/cybersecurity/2021/10/doj-hit-government-contractors-very-hefty-fines-if-they-fail-disclose-data-breaches/185894/. The DOJ and qui tam relators have pursued a number of cases involving noncompliance with Government contract cybersecurity requirements. Below are summaries of some of the most significant cases:

(1) *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245 (E.D. Cal.): A qui tam relator alleged that Aerojet made implied false certifications that it complied with cybersecurity requirements and sought $2.6 billion in damages, exclusive of treble damages, based on the value of Aerojet's Government contracts from 2013–2015. The court denied Aerojet's motion to dismiss, indicating that the relator's allegations stated valid claims under the FCA. *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.,* 381 F. Supp. 3d 1240 (E.D. Cal. 2019); see also *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245, 2022 WL 297093 (E.D. Cal. Feb. 1, 2022) (denying plaintiff's motion for summary judgment and granting defendants' motion for summary judgment in part). The lawsuit settled for $9 million. DOJ Press Release, *Aerojet Rocketdyne Agrees To Pay $9 Million To Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts* (July 8, 2022), https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

(2) *U.S. ex rel. Craig v. Georgia Tech Research Corp.*, No. 1:22-cv-02698 (N.D. Ga.): Two relators, the Associate Director of Cybersecurity and a former student and Georgia Tech employee, filed a qui tam action alleging that Georgia Tech failed to implement NIST SP 800-171 security controls in violation of DFARS 252.204-7012 and made false attestations of compliance with NIST SP 800-171. The DOJ intervened. On October 21, 2024, Georgia Tech filed a motion to dismiss, arguing, among other things, that it was not subject to the claimed DOD cybersecurity requirements, including because the relevant contracts were for fundamental research and did not involve CDI. The case is ongoing.

(3) *U.S. ex rel. Decker v. Penn. State University*, No. 2:22-cv-03895 (E.D. Pa.): The former Chief Information Officer for Penn State's Applied Research Laboratory filed a qui tam action alleging that Penn State failed to comply with NIST SP 800-171 in violation of DFARS 252.204-7012 and violated DFARS 252.204-7020. Penn State and DOJ reached a $1.25 million settlement. DOJ Press Release, *The Pennsylvania State University Agrees To Pay $1.25M To Resolve False Claims Act Allegations Relating to Non-Compliance With Contractual Cybersecurity Requirements* (Oct. 22, 2024), https://www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating.

(4) In 2023, Verizon Business Network Services LLC and the DOJ reached a $4 million settlement resolving allegations that Verizon Business Network Solutions failed to meet all cybersecurity requirements under Government contracts for information technology services. DOJ Press Release, *Cooperating Federal Contractor Resolves Liability for Alleged False Claims Caused by Failure To Fully Implement Cybersecurity Controls* (Sept. 5, 2023), https://www.justice.gov/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully.

(5) *U.S. ex rel. Seikop v. Insight Global LLC*, No. 1:21-cv-1335 (M.D. Pa.): Insight Global faced a

qui tam action under the FCA alleging that it violated the FCA "by failing to implement adequate cybersecurity measures to protect health information obtained during COVID-19 contract tracing," including by failing to encrypt personal health information and personally identifiable information. The lawsuit settled for $2.7 million. DOJ Press Release, *Staffing Company To Pay $2.7M for Alleged Failure To Provide Adequate Cybersecurity for COVID-19 Contact Tracing Data* (May 1, 2024), https://www.justice.gov/opa/pr/staffing-company-pay-27m-alleged-failure-provide-adequate-cybersecurity-covid-19-contact.

Takeaways

Contractors face two principal headwinds relating to information security: increased regulation and increased enforcement. Contractors must be vigilant about implementing appropriate information security policies and controls to ensure compliance with contractual obligations and to mitigate bid protest, contract dispute, and FCA liability risks. Thus, contractors must implement required cybersecurity controls, develop policies for handling CUI and other regulated data, create policies for responding to cyber incidents, incorporate information security requirements into subcontracts, verify supply chain compliance, and train employees on compliance obligations. When contractors discover noncompliances, they should investigate the issues; assess whether the mandatory disclosure rule in FAR 52.203-13, "Contractor Code of Business Ethics and Conduct," or other contract clause or FAR provision (e.g., FAR 9.406-2(b)), requires disclosure; and take remedial actions to come into compliance while limiting risks in the interim. *Tom Pettit*