THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 59, No. 7 **February 22, 2017**

Focus

¶ 43

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 2—Looking Beyond The FAR And DFARS—Other Safeguarding And Reporting Requirements

In Part 1, we discussed the cybersecurity requirements applicable to federal contract information under Federal Acquisition Regulation 52.204-21(b)(1) and covered defense information (CDI) under Defense FAR Supplement 252.204-7012, which requires contractor compliance by December 31. See 59 GC ¶ 25. In Part 2, we examine other safeguarding and reporting requirements for unclassified information, including agency-specific regulations, of which Government contractors should be aware. Many of these requirements have been in place for years, and your company may already have plans and processes for compliance. However, it is worth reexamining these requirements and considering the data and systems they affect, as well as how security may be improved when planning for compliance with the DFARS rule by December 31.

Agency-Specific Regulations—There is a vast web of agency-specific regulations related to cybersecurity to which contractors may be subject. Obviously, contractors should review in detail their contracts to understand agency-specific requirements and coordinate with their customers regarding cybersecurity expectations.

As outlined below, many agencies have security requirements in place for protecting *unclassified* technology resources that may require contractors to produce an information technology "security plan," provide security training, and maintain procedures for detecting and reporting security incidents. Below we summarize a few such agency-specific regulations.

Department of State (DOS): DOS Acquisition Regulation (DOSAR) § 652.239-71—This clause notes that contractor failure to comply could result in contract termination. 48 CFR 652.239-71(m).

Applicability—The regulation applies "to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOS's information that directly supports the mission of DOS." Id. at (a).

- *Note*: The regulation includes a mandatory flow-down provision requiring the contractor to incorporate the substance of the clause in all subcontracts that meet the conditions included in paragraph (a) of the clause. Id. at (k).

IT Security Plan—The contractor must submit for acceptance by the contracting officer and the CO's representative an IT security plan within 30 days after contract award. Id. at (c). The plan must comply with the Federal Information Security Management Act, the E-Government Act, Office of Management and Budget Circular A-130, National Institute of Standards and Technology Standard Publication 800-37, and certain sections of the DOS Foreign Affairs Manual and Foreign Affairs Handbook. Id. at (b).

- *Practitioner's Note*: The plan, as accepted, is to be incorporated into the contract as a compliance document. Id. at (c). Thus, there could be a risk of "implied certification" False Claims Act liability for invoices submitted in the face of a "knowing" failure to follow the IT security plan.

Accreditation—The contractor shall, within six months after contract award, submit for acceptance by the CO proof of IT security accreditation in accordance with NIST SP 800–37. The accreditation is to be incorporated into the contract as a compliance document. Id. at (d).

Verification—The contractor must submit annually to the CO verification of the continuing validity of the IT security plan. Id. at (e).

Privacy Act Notification—The contractor is to display a notice on all DOS systems containing Privacy Act information that is visible prior to allowing anyone to access the system. Id. at (g). (See below for more detail on the Privacy Act.)

Training—Contractor employees must receive annual IT security training in accordance with OMB Circular A-130, FISMA and NIST requirements. Id. at (i).

Department of Homeland Security (DHS): DHS Acquisition Regulation (HSAR) § 3052.204-70

Applicability—This regulation applies to contracts that include "information technology resources or services for which the contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission." 48 CFR 3052.204-70(a).

IT Security Plan—The contractor shall submit an IT security plan within a certain number of days to be specified by the agency. The plan must be in compliance with FISMA, the Computer Security Act, the Government Information Security Reform Act and OMB Circular A-130. The plan is to be approved by the CO and incorporated into the contract as a compliance document. Id. at (b). See the practitioner's note above regarding potential FCA liability arising out of this requirement.

Accreditation—The contractor shall submit proof of IT security accreditation based on the criteria of DHS Sensitive System Policy Publication 4300A (or a replacement publication) within six months after contract award for approval by the CO. Id. at (d).

DHS proposed rules published on January 19 would expand security and privacy requirements for contractors. The proposed rules include new requirements for (1) handling controlled unclassified information (CUI) and related incident reporting (see HSAR Case 2015-001); (2) IT security awareness training for all contractor and subcontractor employees with access to DHS or contractor systems "capable of collecting, processing, storing or transmitting [CUI]" (see HSAR Case 2015-002); and (3) a standardized HSAR regulation for training on privacy and the handling of personally identifiable information (PII) (see HSAR Case 2015-003). Comments on the proposed rules are due by March 20.

General Services Administration (GSA): General Services Acqusition Manual § 552.239-71—This clause is similar to the DOS regulation and provides, similarly, that a failure on the part of the contractor to comply could result in contract termination. 48 CFR 552.239-71(n).

Applicability—The regulation applies "to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to GSA's information that directly supports the mission of GSA, as indicated by GSA." Id. at (a).

- *Note*: The regulation includes a mandatory flow-down provision requiring the contractor to incorporate the substance of the clause in all subcontracts that meet the conditions included in paragraph (a) of the clause. Id. at (l).

IT Security Plan—Within 30 days after contract award, the contractor shall submit an IT security plan for acceptance by the CO and COR. Id. at (c). The plan must comply with FISMA, the E-Government Act and GSA policies, including the "CIO IT Security Procedural Guide 09-48, Security Language for Information Technology Acquisitions Efforts." Id. at (b). It is to be incorporated into the contract as a compliance document. Id. at (c).

Authorization—The contractor shall submit proof of IT security authorization in accordance with NIST SP 800-37 within six months after contract award for acceptance by the CO. The accreditation is to be incorporated into the contract as a compliance document. Id. at (e).

Verification—The contractor must submit to the CO an annual verification regarding the continuing validity of the IT security plan. Id. at (f).

Privacy Act Notification—The contractor is to display a notice on all GSA systems containing Privacy Act information that is visible prior to allowing anyone to access the system. Id. at (h).

Training—Contractor employees must receive annual IT security training in accordance with OMB Circular A-130, FISMA and NIST requirements. Id. at (j).

Department of Veterans Affairs (VA): The VA's cybersecurity clause, VA Acquisition Regulation 852.273-75, was suspended in 2012. VA Handbook 6500.6, Contract Security, is to be used in lieu of the suspended clause. VA Handbook 6500.6 provides the following:

Applicability—This guidance applies to contractor systems that store, generate, transmit or exchange VA sensitive information in a contractor-developed and -maintained system.

Accreditation—Contractor systems are to be certified and accredited in compliance with VA policy (pursuant to the checklist provided in Appendix A to VA Handbook 6500.6) and VA Handbook 6500.3, Certification and Accreditation of VA Information Systems.

Training—Contractors are to complete security and privacy training as outlined in Appendix C of the VA Handbook.

The above agency-specific rules are only a handful of many. For any contractor systems that touch unclassified Government information, contractors should ensure the appropriate safeguards are in place in accordance with their contracts and other agency-specific requirements.

Data-Specific Requirements—CUI—*National Archives and Records Administration (NARA) Rule Regarding CUI*: The FAR final rule discussed in Part 1, FAR 52.204-21, provides "basic" requirements for safeguarding federal contract information. These basic requirements encompass 15 standards relating to six of the 14 security control families in NIST SP 800-171. The DFARS rule covered in Part 1 requires compliance with the standards in all 14 NIST SP 800-171 security control families by December 31. As discussed in Part 1, the definition of CDI under the DFARS final rule is tied to the CUI Registry. See DFARS 252.204-7009 (81 Fed. Reg. 72998).

NARA enacted a final rule, effective Nov. 14, 2016, setting forth requirements for "Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency." 81 Fed. Reg. 63324. (The final rule notes that "[a]gencies and their contractors should already be complying with the authorities governing CUI." The rule merely "gathers a majority of CUI under one set of consistent requirements … and standardizes how agencies comply throughout the executive branch." Id. at 63327–63328.)

The rule contemplates situations in which a contractor uses or stores information "on behalf of" an agency, in which case NIST 800-53 will apply, as well as situations such as those discussed in Part 1, in which a contractor is "not using or operating an information system or maintaining or collecting federal information 'on behalf of' an agency." Id. at 63330. Where the contractor is not acting on behalf of an agency, synonymous with the DFARS rule, the NARA final rule states agencies are to "prescribe the requirements of NIST SP 800-171 in agreements to protect the confidentiality of the CUI, unless the agreement establishes higher security requirements." Id. Under this rule, agencies are to "extend the controls for handling CUI to contractors by means of contract provisions." Id. at 63332.

The rule makes it clear that agencies still are free to promulgate agency-specific policies regarding CUI. Id. at 63326. Thus, not only are contractors required to implement by December 31 the security controls in NIST SP 800-171 under the DFARS final rule for safeguarding information, but contractors that have access to CUI or may handle CUI under a contract with any executive agency also will be expected to understand and implement the security controls at NIST SP 800-171. See Part 1, 59 GC ¶ 25. The NARA final rule promises a "new FAR case on CUI" that is in the process of being drafted. 81 Fed. Reg. 63332 ("[T]he CUI EA is developing a Federal Acquisition Regulation (FAR) case through the normal FAR process, for agencies to use in contracts, which will further reduce chances of overreach." Id. at 63328).

Comments discussed in the NARA final rule address contractors' responsibilities to identify CUI even when not properly marked by an agency, which could shed light on how such situations will be handled under the DFARS final rule. The NARA final rule states,

> If a contractor receives improperly marked CUI from an agency, the contractor is not responsible for having marked the CUI improperly, but the contractor could be responsible for knowing the types of CUI it receives from the agency pursuant to the contract, and for knowing which CUI Registry category the information falls into, the handling requirements for that type of CUI, and so forth. As a result, the contractor could, in some cases, also be held responsible for properly handling the CUI even if it is not marked properly when they receive it.

The NARA rule essentially makes the contractor potentially responsible for agency negligence or misfeasance. This approach seems on its face to be unfair and unreasonable, not only for this reason, but also because it deprives contractors of predictability of outcome in this critical area. To put it bluntly, how are contractors to categorize information when the Government—the generator and transmitter of the information—is unable to do so?

Data-Specific Requirements—PII—*The Privacy Act*: The Privacy Act, 5 USCA § 552a, regulates the collection, maintenance, use and dissemination of personal information by federal executive branch agencies and certain contractors. It applies to all contracts "for the operation by or *on behalf of the agency* of a system of records to accomplish an agency function." 5 USCA § 552a(m)(1) (emphasis added). It also applies to contracts under the supervision, control or oversight of the agency, and to contracts that require compliance with the Privacy Act. See *Shannon v. Gen. Elec. Co.*, 812 F. Supp. 308, 313, 315 n.5 (N.D.N.Y. 1993) ("no dispute" that the contractor is an "agency" subject to requirements of Privacy Act where, pursuant to contract, it operated Department of Energy-owned lab under DOE supervision, control and oversight, and whereby terms of contract it agreed to comply with Privacy Act).

Contract language signaling that the Privacy Act applies to a contract may read as follows:

> The Contractor is bound by Section (m) of the Privacy Act, 5 U.S.C. Sec. 552a(m), and as such is considered under the act to be an employee of the agency. Accordingly, the Contractor and any of its employees are subject to the criminal penalties of the Privacy Act, 5 U.S.C. Sec.552a(i).

Where applicable, contractors are restricted from disclosing PII to unauthorized persons or accessing PII on unauthorized devices. Contractors violating the Act may be subject to criminal penalties.

PII is information that contains a unique identifier (e.g., a name or Social Security number) or information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. Other examples may include a driver's license number or identification card number, date of birth, home address, e-mail address, and financial account numbers.

Because the definition of PII is not anchored to any single category of information or technology, contractors must do a case-by-case assessment of the specific risk that an individual may be identifiable from the information. NIST provides the following illustration: "[A] list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual. … [I]f the list of credit scores were to be supplemented with information, such as age, address, and gender, it is probable that this additional information would render the individuals identifiable." See NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), at 2-1, n.18 (April 2010).

Note that definitions for "personal information" differ among states. In certain states, login credentials such as usernames, e-mail addresses and passwords are considered personal information. See Cal. Civ. Code § 1798.82; Fla. Stat. Ann. § 501.171; 815 Ill. Comp. Stat. 530/1 to 40; Neb. Rev. Stat. §§ 87-802 to 804; N.D. Cent. Code §§ 51-30-01 to 07; Nev. Rev. Stat. Ann. §§ 603a.010, .220; R.I. Gen. Laws §§ 11-49.3-3 to 5; Wyo. Stat. Ann. §§ 40-12-501 to 502. Additionally, biometric data (e.g., fingerprint, retina or iris "measurements"), see, e.g., 815 Ill. Comp. Stat. 530/5, or "[i]nformation or data collected through the use or operation of an automated license plate recognition system," may be "personal information." See Cal. Civ. Code §§ 1798.29, 1798.90.5.

Privacy Training Rule (FAR Case 2010–013): Effective January 19, a final rule requires all contractors and subcontractors with "access to a system of records on individuals or [who] handle PII"—regardless of contract type or value—to train employees on the Privacy Act requirements and penalties for violations, including,

- handling and safeguarding of PII;
- authorized use of PII and a system of records;
- prohibited use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access PII;
- prohibited use of a system of records or unauthorized disclosure, access, handling or use of PII; and
- incident response procedures for suspected or confirmed breaches of a system of records or unauthorized disclosure, access, handling or use of PII.

FAR 52.239-1, Privacy or Security Safeguards (the "Privacy Act clause"): FAR 52.239-1 implements the Privacy Act, 5 USCA § 552a, and requires that certain contractors that process, store, or maintain PII on behalf of the Government report breaches of PII to the Government. The reporting requirement, however, is limited to contracts "which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services." See FAR 39.106 (while nothing in the

plain language of FAR 52.239-1 prohibits it from being incorporated in non-IT contracts, there is no case law or legislative history to suggest that the Government will apply FAR 52.239-1 to a non-IT contract).

"The term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 USCA § 552a(a)(5). Note the regulation does not apply where the contract merely involves records. See *Koch v. Schapiro*, 777 F. Supp. 2d 86, 91 (D.D.C. 2011) (concluding that "a contract to investigate complaints of discrimination by employees of the agency on behalf of the [agency's equal employment opportunity] Office" is "not a contract for the design or development of a system of records," and is not the type of contract covered by FAR pt. 24, Protection of Privacy and Freedom of Information). Where FAR 52.239-1 applies, contractors must "immediately" notify the Government if (1) "new or unanticipated threats or hazards are discovered," or (2) "existing safeguards have ceased to function."

Additional notification requirements for PII such as those below also may apply:

GSA Information Breach Notification Policy (GSA Order, CIO 2100.1J (Dec. 22, 2015))—Contractors must report all incidents involving known or suspected breaches of PII within *one hour* of discovering the incident. Reports should be made to the contractor's information systems security officer (ISSO) and the Office of the Senior Agency Information Security Officer (OSAISO). Where the ISSO cannot be reached, the information system security manager and OSAISO should be contacted.

State Breach Notification Statutes—If PII is compromised, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require companies to notify consumers and possibly credit reporting agencies, state regulators, and attorneys general, but the requirements vary widely. (Alabama, New Mexico and South Dakota do not require this.) In addition to the definition of "personal information," state laws may differ on (1) applicability (e.g., businesses, information brokers, Government entities); (2) who must be notified (e.g., consumers, credit reporting agencies, state attorneys general); and (3) when the notification requirement is triggered. State "safe harbors" relating to notification requirements for encrypted data also are inconsistent. For example, Virginia defines encryption as "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." Va. Code Ann. § 18.2-186.6. This is the same standard used in the Health Insurance Portability and Accountability Act security rule. 45 CFR 164.304. In contrast, Rhode Island specifies that the "algorithmic process" for encryption must be 128-bit or higher and indecipherable "without use of a confidential process or key." R.I. Gen. Laws § 11-49.3-3(a)(2).

- California has one of the broadest consumer-protection statutes. Not only does California require notice to any affected resident, but, in January 2017, California amended its statute to require anyone conducting business in California to disclose both actual and *suspected* breaches. See Cal. Civ. Code § 1798.29(a) (agency requirement), § 1798.82(a) (person or business).
- *Practitioner's Note*: Contractors should identify breach notification requirements *before* an incident occurs. The statutes and regulations often provide specific content and formatting requirements for notifications (e.g., headings, font size). Instead of identifying these details mid-crisis, contractors should prepare templates for each state's requirements. An incident response plan should outline the applicable state laws, including the required content for notices and any agency reporting requirements. Because the laws are constantly changing, the contractor's incident response plan also should identify the frequency with which applicable state statutes and notification requirements will be reevaluated. The notice templates should be updated accordingly.

The Family Educational Rights and Privacy Act (FERPA): FERPA prohibits the unauthorized disclosure of students' PII. 20 USCA § 1232g; 34 CFR Pt. 99. Contractors that receive federal funding through the Department of Education or maintain, transmit or store students' information on behalf of an educational agency are subject to FERPA.

Data-Specific Requirements: Health Information and Medical Devices—*HIPAA Security Rule*: 45 CFR pt. 160 and subpts. A and C of pt. 164. Under the HIPAA security rule, covered entities and business associates receiving, creating, maintaining, or transmitting electronic protected health informa-

tion (PHI) are required to implement administrative, physical and technical safeguards to prevent the unauthorized use, disclosure, integrity and availability of the data. The security rule establishes minimum security requirements, but emphasizes that security measures must be "reasonable" based on an initial and ongoing risk assessment.

PHI includes individually identifiable health information relating to (a) an individual's past, present or future physical or mental health or condition; (b) the provision of healthcare to an individual; or (c) the past, present or future payment for the provision of healthcare to an individual.

Contractors offering medical services or medical devices to the Government will be subject to the HIPAA security rule. HIPAA language in a VA contract for medical services might appear as follows:

> The Contractor personnel herein agree to take all reasonable precautions to safeguard patient information from unauthorized access or modification, in both electronic and hard-copy formats. This includes not only electronic security measures such as "strong" user passwords on computer systems, but also physical barriers to prevent unauthorized use of computer workstations; that hard copy Veteran Residents files are in secured lockable areas, that files are in lockable cabinets, that the cabinets can in fact be locked (i.e., keys are available, and the locking mechanisms work properly). This precaution also includes the proper transfer of Veteran Resident information via electronic means, such as faxing or system-to-system transmission.

Health Information Technology for Economic and Clinical Health (HITECH) Act: 42 USCA § 17921—This law applies to entities with access to unsecured PHI. Entities that have experienced a data breach must notify affected individuals as well as the Department of Health and Human Services. Notification generally must be provided to individuals within 60 days of discovery of the breach. See 42 USCA § 17932(d)(1). HHS must be notified *immediately* if a breach affects more than 500 people, and the media must be notified if 500 or more affected individuals are within the same state or jurisdiction (42 USCA § 17932(e)(2)–(3)). Breaches affecting fewer than 500 people are to be logged and reported to HHS annually (42 USCA § 17932(e)(3)). Failure to comply with notification requirements subjects contractors to HHS, Office for Civil Rights (OCR)'s compliance authority and state attorneys general who may bring suit on behalf of their residents to enforce the HITECH Act. See 42 USCA § 1320d-5(d).

Medical Device Reporting (MDR) Regulation: 21 CFR Pt. 803. Medical devices, which now may include mobile apps, are regulated by the Food and Drug Administration. The FDA approves medical devices only if there is "a reasonable assurance that the benefits to patients outweigh the risks." The MDR regulation contains mandatory requirements for manufacturers, importers, and device user facilities to report certain device-related adverse events as well as product problems. See 21 CFR Pt. 803.

Data-Specific Requirements—Customer Data—Publicly traded contractors subject to Securities and Exchange Commission jurisdiction must safeguard customer data and disclose to investors any "material" cybersecurity risk or incident. See CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011); Securities Act Rule 408; Exchange Act Rule 12b-20; Exchange Act Rule 14a-9. Information is "material" where "there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available." CF Disclosure Guidance: Topic No. 2, Cybersecurity n.3.

Conclusion—There are myriad cybersecurity-related laws and regulations that contractors should monitor and understand. We have summarized just a sampling of the requirements that may apply to contractors, and so this is not to be viewed as exhaustive or as a substitute for seeking professional representation specific to your situation. This year, as plans are solidified for compliance with the DFARS rule for safeguarding CDI by December 31, contractors should take the opportunity to review their systems and data as well as their contracts to facilitate better security in accordance with agency-specific requirements and other data-specific rules. Plans and procedures for monitoring contractor systems and acknowledgement of applicable reporting requirements should be part of this process.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* John Chierichella, Laura Jehl, Townsend Bourne *and* Melinda Biancuzzo. *Mr. Chierichella is a partner in the Washington, D.C. office of Sheppard, Mullin, Richter & Hampton, a member of the firm's Government Con-

tracts, Investigations, and Internal Trade practice group, and co-leader of the firm's Aerospace and Defense Industry team. Ms. Jehl is a partner in the firm's Business Trials practice group and co-leader of the Privacy and Cybersecurity team. Ms. Bourne and Ms. Biancuzzo are associates in the firm's Government Contracts, Investigations and Internal Trade practice group. They can be reached at jchierichella@sheppardmullin.com, ljehl@sheppardmullin.com, tbourne@sheppardmullin.com and mbiancuzzo@sheppardmullin.com, respectively.

