THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

THOMSON REUTERS®

Vol. 59, No. 37 October 11, 2017

In this issue ...

Focus

¶ 306

FEATURE COMMENT: Lurking In The NIST—Why Federal Contractors May Be Misreading Their Cybersecurity Safeguarding Requirements

Introduction—If your company sells products or services to the U.S. Government, there's a substantial likelihood that you've read or heard the acronym "NIST" in connection with various cybersecurity-related obligations that the Government is imposing on contractors with a seemingly unceasing vengeance. NIST refers to the National Institute of Standards and Technology, which is a nonregulatory agency of the Department of Commerce, and which has the stated mission of promoting "U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

With the Federal Information Security Modernization Act of 2014, NIST became statutorily vested with various responsibilities, the most central of which requires the development of information security standards and guidelines, including minimum requirements for federal information systems that do not relate to national security systems. 44 USCA § 3553(h)(2)(E), (G). In furtherance of this mandate, NIST has propounded certain special publications (SPs) that function as technical blueprints against which the sufficiency of contractors' information systems are—as a matter of regulation—measured. Perhaps the most prominent (or *notorious*) SP is NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

As most of us know, the requirements of NIST SP 800-171 now percolate into virtually every contract with the Department of Defense pursuant to Defense Federal Acquisition Regulation Supplement clause

Focus continued on page 3 ...

✦ Index ✦

Focus

Developments

Decisions

— Case Table —

252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, via DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls. What many fail to realize, however, is that provisions of 800-171 and the safeguarding requirements in DFARS 252.204-7012 are not synonymous.

Rather, as described below, 800-171 is a piece of DFARS 252.204-7012 and codifies some—but not all—of the DFARS requirements that must be met. Far from all-inclusive, 800-171 addresses only the *confidentiality* of the Government's data. It does not address, nor is it intended to encompass, data *integrity* or *availability*. Although authors, commenters and consultants are happy to discuss the basic, checklist-like nature of 800-171 confidentiality requirements, most fail to analyze the full scope of 7012 and the requirements that contractors must meet to provide the "adequate security" necessary if possessing or handling "covered defense information" (CDI) in connection with the performance of a federal contract. See, e.g., DFARS 252.204-7008(b) ("The security requirements required by contract clause 252.204-7012 shall be implemented for all [CDI] on all covered contractor information systems that support the performance of this contract.").

Yes, what we're saying is that these "experts" can't see through the NIST and may be leaving contractors exposed to legitimate Government or competitor claims that they are failing to abide by the contractual requirements of DFARS 252.204-7008 and -7012. The purpose of this Feature Comment is to help elucidate the full scope of the DFARS -7012 safeguarding requirements, and, in so doing, provide clearer insight into the intent of 800-171 while imparting some wisdom from the trenches to ensure that you are cybersecure.

A Deeper Look at DFARS 252.204-7012 "Safeguarding": There's a Monster under the B…—Before diving into SP 800-171, it is a good idea to understand why we are even discussing it. As described briefly above, 800-171 is incorporated into the DFARS clause found at 252.204-7012. For the uninitiated—or for the understandably confused—DFARS 252.204-7012 is a clause typically found (whether it belongs there or not) in most contracts and subcontracts relating to DOD acquisitions.

It addresses two primary concerns related to the possession and transmission of DOD data: (1) safeguarding and (2) incident reporting. In a perfect world, if you are doing #1 right, then #2 becomes superfluous. If only the world were perfect.

The clause provides, with seeming aspiration, that incident reporting can be avoided by DOD demanding that contractors provide "*adequate security* on all *covered contractor information systems*." DFARS 252.204-7012(b). The clause defines both italicized phrases:

- *Adequate security* means protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to, or modification of, information.
- *Covered contractor information system* means an unclassified *information system* that is owned or operated by or for a contractor and that processes, stores or transmits *CDI*.

Since we're dealing with a federal regulation, these definitions include embedded definitions to ensure that their meanings and intent remain somewhat confusing. So, in an effort to examine the clause fully, we'll need to define a few other phrases:

- *Covered defense information* (*CDI*) means unclassified *controlled technical information* or other information, as described in the Controlled Unclassified Information (CUI) Registry at *www.archives.gov/cui/registry/category-list.html*, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations and Government-wide policies, and is—
  (1) marked or otherwise identified in a contract, task order or delivery order, and provided to the contractor by or on behalf of DOD in support of contract performance; or
  (2) collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of contract performance.
- *Information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- *Controlled technical information* means *technical information*, with military or space application, that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure or dissemination.

Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F in DOD Instruction 5230.24, Distribution Statements on Technical Documents. The phrase does not include information that is lawfully publicly available without restrictions.

- *Technical information* means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether the clause is incorporated in a specific solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Now, with all of the key phrases identified, and since it's almost Halloween, let's cobble together what it actually means to provide "adequate security on all covered contractor information systems" using these definitions, à la the work of Dr. Frankenstein:

(b) *Adequate security*. The Contractor shall provide protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information on all unclassified discrete set[s] of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information that is owned, or operated by or for, a contractor and that processes, stores, or transmits unclassified technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract (e.g. research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code) with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination, (inclusive of instances if disseminated, for distribution statements B through F using the criteria set forth in DOD Instruction 5230.24, Distribution Statements on Technical Documents, but exclusive of information that is lawfully publicly available without restrictions), or other information, as described in the Controlled Unclassified Information (CUI) Registry at *www.archives.gov/cui/registry/category-list.html*, that:

- Requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is
- 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
- Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Now that's a monster! And it is just the first sentence of DFARS 252.204-7012(b). It is not surprising that, even before examining the specifics of "how to do it all," the assessment of "what all to do" has many federal contractors quaking in their choice of comfortable footwear. In fact, it probably took you a couple of tries to read through the whole, expanded clause. If not, re-read it, and this time look for NIST. Don't worry, you're not going blind, it's not in there—providing "adequate security" under the DFARS imposes requirements that are not, necessarily, NIST-based.

Keeping that lumbering monstrosity of *what* needs to be protected in the rearview for just a minute, let's next take a look at *how* DOD expects contractors to provide that adequate security (notice we did not say "safeguard"). For the sake of brevity (and conceding the shortness of life), we'll examine the requirements of "covered contractor information systems that are not part of an [information technology] service or system operated on behalf of the

Government." DFARS 252.204-7012(b)(2). For our purposes here, let us describe these systems generally as external contractor systems, and in accordance with the definition of "covered contractor information system" identified above, we note that the clause requires, "at a minimum," that:

> Any unclassified *information system* that is owned, or operated by or for, a contractor and that processes, stores, or transmits *covered defense information* is subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

DFARS 252.204-7012(b)(2)(i). And there it is! NIST SP 800-171—the "security requirements" that will be subjected against your information system. The protections that, "at a minimum," must be implemented to provide "adequate security," and, if we're being honest, are necessary to avoid a parade of horribles (think terminations for default, False Claims Act allegations, breach of contract complaints, etc.). Get the pencils out, and let's check these things off the list to be "800-171 compliant" (whatever that is). As we all know, we do not have long—the December 31 deadline is just around the corner.

If this were a horror movie, that would be the end of Act 1, the point in the movie where the plucky hero avoids the monster and thinks she's in the clear. But we know better, don't we? This movie is just beginning.

The clause found at DFARS 252.204-7012(b)(3) addresses what is best described as the "catch all." Stated simply, and with great apparent deference to contractors, the clause directs contractors to

> [a]pply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment *or* to accommodate special circumstances (e.g., medical devices) *and* any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

Fear resides in the unknown and, for federal contractors, that cybersecurity unknown is stated humbly at DFARS 252.204-7012(b)(3). Not only is there no guidance on what these "other information systems security measures" should be, there is no direction on how or when they should be used. Rather, the clause directs only that they be employed to "provide adequate security in a dynamic environment." In our experience, this "dynamic environment" incorporates future risks and threats, such as connected devices found on the "internet of things," and vulnerabilities that may only become apparent upon your adversaries' successes or your vendors' failures, if you're lucky.

We get the sense that many contractors stumbling through the cybersecurity darkness are using 800-171 compliance (whatever that is) like a silver cross, wolfsbane or a necklace of garlic—believing that it will ward off, if not they who rule the dark(web)—the regulators who may knock on their doors. That is not the case.

As stated in the regulation, contractors must provide "adequate security" on their covered systems. This means contractors must provide "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information." This, NIST SP 800-171 does not do. And don't take our word for it. NIST SP 800-171 itself is clear that providing "adequate security" was never its goal.

A Deeper Look at NIST SP 800-171: De-NIST-ifying Cybersecurity—It is worth noting at the outset that we believe NIST SP 800-171 does what it was intended to do—e.g., to provide

> federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

NIST SP 800-171, Rev. 1, Abstract, December 2016. In this regard, 800-171 is a great document that provides federal agencies with clear expectations on how to protect Government data confidentiality. However, the Government demands more from con-

tractors than simply keeping its data confidential. It also expects that Government data integrity and availability are maintained. Federal Information Security Management Act of 2002, 44 USCA § 3544. This means that in addition to maintaining the confidentiality of data, the law also requires agencies to ensure that data are guarded "against improper information modification or destruction," and that the Government is ensured "timely and reliable access to and use of information." 44 USCA § 3542.

The elements of data integrity and data availability are key to the Government's information security efforts. Both are central to NIST's Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," and 200, "Minimum Security Requirements for Federal Information and Information Systems," along with NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations." All three documents reference data integrity and availability alongside confidentiality as the variables needed to craft the proper security for Government information systems and the data they hold.

However, as it plainly concedes, 800-171 is spawned from "tailoring criteria applied to the FIPS Publication 200 security requirements and the NIST Special Publication 800-53" that focus "on the protection of CUI from unauthorized disclosure in nonfederal systems and organizations." NIST SP 800-171, Rev. 1, Cautionary Note, December 2016. It is for this reason that 800-171 cautions that "organizations should not assume that satisfying those particular requirements will automatically satisfy the security requirements and controls in FIPS Publication 200 and Special Publication 800-53." Id.

Put more succinctly, "the primary purpose of this publication is to define requirements to protect the confidentiality of CUI." The publication goes on to note that although "there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives," it advises organizations that are "required to comply with the recommendations in this publication" to examine other controls "to ensure that their individual security plans and security control deployments provide the necessary and sufficient protection to address the cyber and kinetic threats to organizational missions and business operations." Id.

If you take the time to review the 800-171 security requirements, it becomes apparent that many cybersecurity requirements are unaddressed. Alternatively, should you not have the time or inclination to read the whole thing, you can turn to Chapter 2 and see that, with a few exceptions, the areas of "contingency planning, system and services acquisition, and planning requirements are not included within the scope of this publication due to the aforementioned tailoring criteria." NIST SP 800-171, Rev. 1, Chapter 2.2, Development of Security Requirements, December 2016. But that is not all.

There are additional gaps that were incised out of SP 800-53 and FIPS Publication 200 that are worth noting. They were removed because "the control or control enhancement is not directly related to protecting the confidentiality of CUI; or … is expected to be routinely satisfied by nonfederal organizations without specification." NIST SP 800-171, Rev. 1, Appendix E, Tailoring Criteria, December 2016. It is important to note that last sentence and the assumption upon which it relies. NIST 800-171 is not all-encompassing because the drafters expect the controls to already be "included as part of an organization's comprehensive security program." Id. The question that contractors must ask themselves then is: Are we meeting these expectations?

For your convenience, please find below a chart intended to help ensure that you have in place (1) controls not directly related to confidentiality of CUI, and (2) controls expected to be routinely satisfied.

Upon reading this, we imagine the exasperated contractor or compliance official who has spent a good portion of this year preparing to be "800-171 compliant" (whatever that is), after a round of expletives, may contest this chart with a guffaw and claim that, since these are SP 800-53 controls, they apply only to the Government and not to federal contractors. Unfortunately, that's not the case.

These controls apply to the Government's data and, more fundamentally, they are meant to ensure that you, as a contractor, are providing "[protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information] on all covered contractor information systems." DFARS 252.204-7012(b). If you are one of those professionals, there are some actions you can take now to ensure that you see through the NIST security

Controls Not Directly Related To Confidentiality Of CUI	Controls Expected To Be Routinely Satisfied
SOFTWARE USAGE RESTRICTIONS	ACCESS CONTROL POLICY AND PROCEDURES
CONTINGENCY PLANNING POLICY AND PROCEDURES	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
CONTINGENCY PLAN	SECURITY TRAINING RECORDS
CONTINGENCY TRAINING	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
CONTINGENCY PLAN TESTING	AUDIT STORAGE CAPACITY
ALTERNATE STORAGE SITE	AUDIT RECORD RETENTION
ALTERNATE PROCESSING SITE	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
TELECOMMUNICATIONS SERVICES	SYSTEM INTERCONNECTIONS
INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	INTERNAL SYSTEM CONNECTIONS
DEVICE IDENTIFICATION AND AUTHENTICATION	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
TIMELY MAINTENANCE	CONFIGURATION MANAGEMENT PLAN
POWER EQUIPMENT AND CABLING	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
EMERGENCY SHUTOFF	INCIDENT RESPONSE POLICY AND PROCEDURES
EMERGENCY POWER	INCIDENT RESPONSE PLAN
EMERGENCY LIGHTING	SYSTEM MAINTENANCE POLICY AND PROCEDURES
FIRE PROTECTION	MEDIA PROTECTION POLICY AND PROCEDURES
TEMPERATURE AND HUMIDITY CONTROLS	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
WATER DAMAGE PROTECTION	ACCESS CONTROL FOR TRANSMISSION MEDIUM
DENIAL OF SERVICE PROTECTION	VISITOR ACCESS RECORDS
SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	DELIVERY AND REMOVAL
SPAM PROTECTION	SECURITY PLANNING POLICY AND PROCEDURES
INFORMATION INPUT VALIDATION	RULES OF BEHAVIOR
ERROR HANDLING	INFORMATION SECURITY ARCHITECTURE
	PERSONNEL SECURITY POLICY AND PROCEDURES
	ACCESS AGREEMENTS
	THIRD-PARTY PERSONNEL SECURITY
	PERSONNEL SANCTIONS
	RISK ASSESSMENT POLICY AND PROCEDURES
	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
	ALLOCATION OF RESOURCES
	SYSTEM DEVELOPMENT LIFE CYCLE
	ACQUISITION PROCESS
	INFORMATION SYSTEM DOCUMENTATION
	EXTERNAL INFORMATION SYSTEM SERVICES
	DEVELOPER CONFIGURATION MANAGEMENT
	DEVELOPER SECURITY TESTING AND EVALUATION
	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
	PROCESS ISOLATION
	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
	MEMORY PROTECTION

requirements and meet the full DFARS safeguarding requirements.

Fully Complying with DFARS Cybersecurity Requirements: Seeing beyond the NIST Requirements—While a comprehensive review of each control not included in 800-171 is beyond the scope of this Feature Comment, it is worth pointing out that there are some basic assumptions that NIST makes about federal contractors expected to handle CUI:

- they all maintain information security policies and procedures addressing all 14 of the security requirement families identified in 800-171;
- they all create and maintain security and audit records;

- they all possess an incident response plan;
- they all have plans to address privacy and security architecture, including supporting life cycle and configuration management plans; and
- they all have codes of conduct that address cybersecurity and penalties for failing to abide.

Although each of these assumptions is basic, we suspect that not all contractors who hold CUI, or who expect to interact with CUI, meet NIST's expectations. Similarly, we suspect that because these assumptions are not expressly included in 800-171, contractors in the thralls of making the December 31 deadline may not know that the security infrastructure they are building could be standing on a shaky foundation. Finally, although 800-171 now requires the creation of a system security plan (Security Control 3.12.4), that plan is not expected to replace the security policies and procedures addressing all 14 of the security requirement families identified in 800-171. Rather, as described, the 800-171 system security plan is a more specific document intended to "describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

The other gap that 800-171 does not address, those controls not directly related to the confidentiality of CUI, may be a bit more problematic for contractors and the Government. Fundamentally, the confidentiality requirements associated with 800-171 are intended to stop the "unauthorized disclosure of information." FIPS Publication 199. They are not intended to ensure data integrity and availability.

That is not to say that the 800-171 security requirements cannot address those elements, only that they are not intended to do so. In fact, 800-171 recognizes "there is a close relationship between the security objectives of confidentiality and integrity. Therefore, most [] security controls in the NIST Special Publication 800-53 moderate baseline that support protection against unauthorized disclosure also support protection against unauthorized modification." This means, in NIST's opinion at least, that if you meet your data confidentiality obligations, there's a good chance data integrity is in a good place. Data availability, by contrast, will likely take additional efforts.

Data Integrity: The crux of 800-171's data integrity requirement is located under Security Requirement 3.14, System and Information Integrity, and focuses on monitoring traffic into and out of covered contractor information systems, and providing updated protection from malicious code and software flaws. NIST SP 800-171, Rev. 1, Table D-14, Mapping System and Information Integrity Requirements to Security Controls, December 2016. Although these efforts address whether an intruder was in the system, and perhaps saw the data, they do not address data integrity as a process, or otherwise direct the contractor to ensure the validity and accuracy of the data reviewed or accessed.

There is no requirement in 800-171, for instance, requiring error checking or any type of validation methods. This is important—to the contractor and the Government alike—because poor data integrity is not always the result of a malicious actor. Basic human error, including unintended changes or data altered during transfer from one device to another, or hardware issues such as a hard disk crash, can disrupt data integrity. It is for this reason that the controls addressing integrity are found in SP 800-53 and require agencies to employ "[i]ntegrity-checking mechanisms including, for example, parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools [that] can automatically monitor the integrity of systems and hosted applications." NIST SP 800-53, Rev. 5 [Draft], Security Control SI-7, Software, Firmware, and Information Integrity, August 2017. What exactly a company needs in terms of data integrity will rely on the type of data being held. Your company should, however, be prepared to address the protective measures it intends to take to address "the consequences and probability of ... the modification of information." DFARS 252.204-7012.

Data Availability: Unlike data integrity, data availability is absent from 800-171, and anyone who is using 800-171 as a roadmap to DFARS compliance will find their efforts lacking. If you think about it, information security is worthless if you cannot get to it. It is for this reason that industry respondents to the 2017 SANS Data Protection Survey identified threats like "ransomware" and "denial of service" attacks as two of the top threats to sensitive data. See Sensitive Data at Risk: The

SANS 2017 Data Protection Survey, September 2017, available at *www.sans.org/reading-room/whitepapers/threats/sensitive-data-risk-2017-data-protection-survey-37950*.

Furthermore, as large swaths of the U.S. recover from three massive hurricanes, the concepts of continuity of operations and contingency planning also come to mind. However, none of this is addressed in 800-171—not even the simple measure of *requiring* data backups! (800-171 only notes that if such backups are made, they need to remain confidential.) Again, this is no slight against 800-171, we note it only to demonstrate that to meet the cybersecurity requirements in the DFARS, you need to look beyond 800-171.

Conclusion—No one said or believed that meeting the DFARS requirements for safeguarding CDI would be easy. It is not. There are a host of hurdles that contractors need to clear to meet the mark, with one of the biggest being the security requirements in 800-171. Unfortunately, contractors' efforts cannot stop there. To provide "adequate security" in their contracts, federal contractors must drive through the NIST to ensure that Government data are not only safe, but also are intact and available.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Franklin C. Turner *and* Alexander W. Major, *the Co-Leaders of the Government Contracts and Export Controls Group at McCarter & English, LLP located in the firm's Washington D.C. office. They can be reached at FTurner@McCarter.com and AMajor@McCarter.com.

Developments

¶ 307

Interior IG Flags Deficient Virgin Islands Construction Contracting

There are "serious procurement deficiencies and inconsistencies in how [the government of the U.S. Virgin Islands'] Department of Property and Procurement (DPP) solicited, evaluated, awarded, and administered contracts" for capital-improvement construction projects, the Department of the Interior inspector general reported September 29.

The IG reviewed 12 V.I. capital-improvement projects worth $25 million. It found that "DPP did not follow procurement rules for competitively bidding construction contracts, guarantee that the evaluation and awarding process for contracts was fair, administer contracts in accordance with the Virgin Islands Code (V.I.C.), or plan projects carefully."

DPP did not enter into written contracts with seven construction vendors nor competitively procure those services, the IG said. Two of the seven vendors were awarded contracts by a former V.I. Public Finance Authority executive director, bypassing DPP completely. The IG could not determine whether one other contract was awarded competitively because DPP and the Department of Public Works, after numerous requests, did not provide sufficient documentation.

Based on its review of contract files, the IG found no assurance that DPP's contractor selection process is free from preferential treatment or ensures careful evaluation. DPP did not use formal rankings for construction contract awards, document reasons for selections or verify claims made by contractors in their bids.

The IG found inconsistencies in how DPP handled construction bonds. Some bonds were not sufficient to cover the contract amount, some bonds were not certified, some were issued months after the contractor began performance and a contractor did not submit any bond at all for one project. Poor planning also led to significant cost change and uncertain scopes of work.

The IG made nine recommendations to improve DPP's construction contract awards and administration, including (a) documenting competition for construction services in contract files, including justifications of contractor selections; (b) ensuring that evaluation committees avoid favoritism and the appearance of favoritism; (c) using standardized selection-committee ratings; (d) verifying bidders' claims about past performance, work experience and financial condition; (e) avoiding contracting with vendors that have not submitted performance bonds; and (f) improving pre-solicitation construction planning. The IG also recommended that the V.I. legislature amend 31 V.I.C. § 236a to set

minimum thresholds for performance bonds to limit exposure when contractors do not perform.

The projects the IG reviewed were financed with proceeds from PFA-issued bonds. PFA is a public corporation and autonomous governmental instrumentality, which finances V.I. capital-improvement projects by issuing bonds. The IG flagged the DPP procurement issues in a management alert issued during a broader audit of PFA's financial operations and controls. The main audit concluded that PFA "did not maintain sufficient internal controls to safeguard assets and did not provide reasonable assurance that financial transactions and related reports were accurate, as evidenced by the $50 million in financial reporting discrepancies, conflicts of interest, and the $101.1 million in questionable expenditures we found during our fieldwork."

The IG's management alert on DPP construction contracting is available at *www.doioig.gov/sites/doioig.gov/files/ManagementAdvisory_VIPFA_Public.pdf*; the larger PFA audit is available at *www.doioig.gov/sites/doioig.gov/files/FinalAudit_VIPFA_Public.pdf*.

¶ 308

Census Bureau Sole-Source Contracts Did Not Follow Regulations, Commerce IG Finds

The Census Bureau did not properly award 25 of 28 noncompetitive contracts reviewed by the Department of Commerce inspector general because contracting personnel did not comply with the Federal Acquisition Regulation, the Commerce Acquisition Manual (CAM) or the Census Bureau's pre-award requirements, the IG has reported. The Bureau could have saved as much as $9.3 million, or about 20 percent, in acquisition costs, the IG added. In a separate report, the IG listed Commerce's contract management as one of the key challenges facing the department in fiscal year 2018.

Census Bureau Contracting—The IG determined that the Bureau awarded sole-source contracts without proper supporting documents or approval and did not properly maintain contract files. Specifically, statutory authorities were incorrectly used to justify noncompetitive awards, market research used to justify noncompetitive awards was insufficient, price reasonableness documents lacked rationale, sole-source justifications were missing required content, justifications lacked proper approval authority and there was not sufficient evidence of contract review board decisions, the IG said.

The IG attributed the Bureau's noncompliance with pre-award requirements to "a weak control environment that allows contracting officials to use broad discretion in awarding noncompetitive contracts" and a lack of sufficient acquisition management oversight of noncompetitive contract awards. "While noncompetitive contracts may be necessary in certain cases when only one contractor is capable of delivering needed goods or services, competition is a critical tool for achieving the best return on investment for taxpayers," the IG chided. "The Bureau may have missed opportunities to promote competition, obtain lower prices, support its noncompetitive decisions in the event of award protests, and ensure effective stewardship of taxpayer dollars by not fully complying with FAR, CAM, and its own requirements before awarding these high-risk contracts."

The IG recommended that the Census Bureau (a) strengthen controls and enforce FAR and CAM documentation requirements for planning and justifying noncompetitive acquisitions; (b) reiterate to contracting officers the need to adequately justify sole-source procurements and obtain appropriate levels of approval; (c) require COs to maintain supporting documents in the contract file, including price reasonableness determinations and market research results; (d) properly maintain and safeguard contract files; (e) ensure that contract review boards maintain evidence of meetings, decisions and outcomes; and (f) train contracting personnel to correct the identified deficiencies.

Department-wide Contracting—According to the IG, key challenges facing Commerce in FY 2018 include improving the management of contracts, grants and cooperative agreements; modernizing legacy information technology systems and improving data quality; delivering a timely 2020 Census at a lower cost per household than the 2010 Census; implementing export control reforms and efficiently administering trade enforcement remedies; and ensuring the continuity of environmental satellite observations by transitioning new satellites into service, managing risks in the acquisition and development of next-in-series satellites, and assessing the viability of using commercial data for weather forecasts.

Commerce's "management of contracts, grants, and cooperative agreements has long presented a challenge by virtue of the large amounts of money at stake," the IG pointed out. For example, the department's FY 2016 obligations included $3.2 billion for goods and services related to satellite acquisitions, intellectual property, IT, management of coastal and ocean resources, and construction and facilities management. The department also obligated around $1.4 billion in grants and cooperative agreements in FY 2016.

According to the IG, contracting-related challenges include strengthening processes governing the use of noncompetitive contracts and maximizing the use of competition, developing and maintaining a competent acquisition workforce, improving oversight and monitoring of Minority Business Centers, and fostering high ethical standards. Referring to its audit of the Census Bureau's use of noncompetitive contract awards, the IG pointed out that requirements such as adequately documenting market research and independent Government cost estimates and properly using statutory authorities "are essential in helping to ensure that acquisitions are adequately planned, sole-source awards are properly justified, and prices can be demonstrated to be fair and reasonable."

The IG also pointed out that its "investigations continue to uncover fraud and misconduct related to Commerce contracts and grants." In the past four fiscal years, IG investigations have resulted in $9.9 million in restitutions, fines, seizures and civil settlements, and led to 14 criminal convictions. Commerce "must work harder to foster high ethical standards throughout its federal contracting programs," the IG admonished.

In June, the Government Accountability Office found that the National Oceanic and Atmospheric Administration, a part of Commerce, lacked a strategy for increasing its use of the private sector to perform hydrographic surveys of U.S. territorial waters and the U.S. exclusive economic zone. See 59 GC ¶ 194. Also in June, GAO reported that major satellite acquisition programs at NOAA, NASA and the Department of Defense left the Government with limited recourse in the event of a catastrophic in-orbit failure. See 59 GC ¶ 196(c). In 2016, the IG found that NOAA's plans to upgrade its polar satellites encountered delays and faced risks, and warned of potential data gaps until the planned new satellites are in orbit. See 58 GC ¶ 166(d). Also in 2016, the IG questioned the National Weather Service's oversight of service contracts, finding administrative deficiencies. NWS is a part of NOAA. See 58 GC ¶ 445.

Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2018 is available at *www.oig.doc.gov/OIGPublications/2017-09-29_FY_2018_TMC_final_Secured.pdf*; *Awarding of U.S. Census Bureau Noncompetitive Contracts Did Not Consistently Follow Federal Acquisition Regulations and Commerce Acquisition Policies* is available at *www.oig.doc.gov/OIGPublications/2017-09-22_Census_Sole_Source_Final_Report.pdf*.

¶ 309

Developments In Brief ...

(a) USDA Should Improve Suspension and Debarment Program, IG Says—The U.S. Department of Agriculture has implemented a comprehensive set of suspension and debarment tools following an inspector general audit in 2010 and has an active referral process, but it did not fully implement six of 27 recommendations from the 2010 audit, the USDA IG recently reported. Further, the Office of the Chief Financial Officer (OCFO) needs to improve the suspension and debarment program's oversight, the IG said, noting that 12 of 17 USDA agencies did not fully comply with at least one requirement of USDA's suspension and debarment program. In 2010, the IG determined that USDA had not fully implemented suspension and debarment program requirements. In 2011, the secretary of agriculture established a Suspension and Debarment Council led by the OCFO "to develop and issue procedural guidance and training recommendations to enable the effective implementation of USDA's suspension and debarment procedures," the IG noted. The Council has representatives from each USDA agency. However, the IG determined that "Council members, representing individual agencies, did not enable effective implementation of USDA suspension and debarment regulations." As a result, "three agencies did not consider suspension and debarment for

program participants convicted of fraud and bribery." The IG also found that USDA regulations did not clearly explain Council members' roles and responsibilities and OCFO did not adequately monitor one agency's implementation of a suspension and debarment program. "While OCFO, in cooperation with the Council, established a comprehensive suspension and debarment program for the Department, we found that monitoring of USDA agencies needs improvement to ensure full compliance," the IG concluded. The IG made nine recommendations, including for OCFO to (a) comply with the IG's 2010 recommendations, (b) define roles and clarify allowable suspension and debarment actions, and (c) develop a process to identify non-compliant agencies. *Implementation of Suspension and Debarment Tools in the U.S. Department of Agriculture* is available at *www.usda.gov/oig/webdocs/50016-0001-23.pdf*.

(b) NAVFAC Should Improve Energy-Savings Contract Administration—Naval Facilities Engineering Command (NAVFAC) contracting officers are not properly approving work changes or appointing CO's representatives for utility energy services contracts (UESCs) at Marine Corps Base Camp Pendleton, Calif., the Department of Defense inspector general reported September 28. The IG reviewed 10 UESCs worth $44.6 million awarded in fiscal years 2009–2015. NAVFAC officials properly awarded and justified the UESCs. But for six of the UESCs, contracting officers did not approve scope of work changes before they were implemented, and for nine, COs did not appoint a CO's representative. COs instead relied on a NAVFAC project manager and other officials to monitor contract performance, did not have controls to identify scope of work changes or performance issues, and believed they were not required to appoint CORs for UESCs. Further, Camp Pendleton energy officials did not have a process to track UESC energy conservation, and could not show that "they achieved sufficient energy savings to pay back the $44.6 million investment," the IG said. The IG recommended that NAVFAC (1) direct COs to approve future scope-of-work changes before contractors begin performance, (2) review COs' and other officials' inappropriate approvals for work changes and take any appropriate administrative action, and (3) establish a written agreement on roles and responsibilities with organizations that NAVFAC COs rely on for contract administration. The IG also recommended that Camp Pendleton develop a system to convert energy usage to cost and realized energy savings for UESCs. In 2014, the IG took Army officials at Fort Knox, Ky., to task for poor UESC administration. See 56 GC ¶ 296. *Naval Facilities Engineering Command Southwest and Marine Corps Base Camp Pendleton Officials' Use of Utility Energy Services Contracts* (DODIG-2017-125) is available at *media.defense.gov/2017/Oct/02/2001820889/-1/-1/1/DODIG-2017-125.PDF*.

(c) VA IG Finds Improper Purchase Card Use to Procure Prosthetics—The Veterans Health Administration used Government purchase cards above the micro-purchase limit to obtain commonly used prosthetics, the Veterans Administration inspector general has reported. As a result, "VHA did not leverage its purchasing power by establishing contracts and did not ensure fair and reasonable prices were paid." Specifically, the IG determined that "VHA's reported cardholder prosthetic purchases increased approximately 25 percent from about $1.6 billion to nearly $2 billion" between fiscal years 2012 and 2015, with approximately $863 million, or 43 percent, of that spent on purchases above the micro-purchase limit. The IG estimated that "VHA may have paid higher prices for an estimated $256.7 million in prosthetics purchases during FY 2015 by not establishing contracts." Further, an estimated 53,400 of 87,100 prosthetics procured by purchase cards in FY 2015, or about 61 percent, were obtained through improper payments and unauthorized commitments, resulting in $520.7 million in improper or unauthorized payments, the IG determined. The IG recommended that VHA (a) identify all commonly procured prosthetics

and pursue appropriate contracts, (b) review FY 2015–2016 prosthetic purchases for unauthorized commitments, (c) perform annual reviews, and (d) hold cardholders and approving officials accountable for unauthorized commitments. In June, the IG flagged VHA purchase card use above the micro-purchase limit at the VA Medical Center in Dublin, Ga. See 59 GC ¶ 208(b). In February, the Government Accountability Office estimated that 13 percent of VA micropurchases lacked required documentation, but found little evidence suggesting purchase card fraud. See 59 GC ¶ 52. *Veterans Health Administration: Audit of Purchase Card Use To Procure Prosthetics* is available at *www.va.gov/oig/pubs/VAOIG-15-04929-351.pdf*.

(d) Supreme Court Declines to Address FCA Appeals—The U.S. Supreme Court October 2 denied, without comment, six petitions for writs of certiorari involving False Claims Act issues, thereby leaving the circuit court opinions standing. In *U.S. ex rel. Hayes v. Allstate Ins. Co.*, 853 F.3d 80 (2d Cir. 2017); 59 GC ¶ 130, the Court of Appeals for the Second Circuit held that the FCA's first-to-file bar is not jurisdictional—a split with the Fourth Circuit's decision in *U.S ex rel. Carson v. Manor Care, Inc.*, 851 F.3d 293 (4th Cir. 2017). In *U.S. ex rel. Jackson v. Univ. of N. Texas*, 673 F. App'x 384 (5th Cir. 2016), the Fifth Circuit held that the FCA's six-year statute of limitations, 31 USCA § 3731(b)(1), barred plaintiff's claims. Plaintiff argued that the longer limitations period under § 3731(b)(2) should apply, but the court said that period applies only when the U.S. intervenes. In *In re Nat. Gas Royalties Qui Tam Litig.*, 845 F.3d 1010 (10th Cir. 2017); 59 GC ¶ 42, cert. denied sub nom. *U.S. ex rel. Grynberg v. Agave Energy Co.*, 2017 WL 1881905 (U.S. Oct. 2, 2017), the Tenth Circuit upheld a district court's award of attorney's fees where relator's claims were clearly frivolous and vexatious. Justice Gorsuch did not take part in the consideration of this petition, as he was serving on the Tenth Circuit when it decided the case. In *Victaulic Co. v. U.S. ex rel. Customs Fraud Investigations, LLC*, 839 F.3d 242 (3d Cir. 2016), the Third Circuit held that knowing failure to mark country of origin for purposes of customs duties could be an actionable FCA claim. In *U.S. ex rel. Harper v. Muskingum Watershed Conservancy Dist.*, 842 F.3d 430 (6th Cir. 2016), the Sixth Circuit held that relators failed to plead the scienter necessary to state a reverse FCA claim against a watershed conservancy district. And in Petition for Writ of Certiorari, *U.S. ex rel. Nguyen v. City of Cleveland*, 2017 WL 2591422 (U.S. May 8, 2017), a pro se relator argued, somewhat unclearly, that various judicial actions and inactions were improper in response to relator's efforts to bring the city of Cleveland into compliance with the Clean Air Act.

Decisions

¶ 310

Agency Eliminated Proposal Based On Considerations Not Found In Evaluation Criteria, Comp. Gen. Says

McCann-Erickson USA, Inc., Comp. Gen. Dec. B-414787, 2017 CPD ¶ 300

An agency improperly eliminated a proposal from a competition based on considerations not contemplated by the solicitation's evaluation criteria, the U.S. Comptroller General recently determined.

The Army issued a request for proposals for a full array of advertising and marketing services for a multi-year indefinite-delivery, indefinite-quantity contract. The evaluation criteria were listed in descending order of importance: technical, cost/price, and small business participation. The RFP indicated that the Army would evaluate proposals to ensure the offerors' proposed cost/price was fair and reasonable, realistic, and balanced.

The solicitation identified a two-phase evaluation process. In phase one, written proposals would be evaluated, and in phase two, all "acceptable" proposals would be invited to make an oral presentation. The phase one evaluation established a

substantive written proposal evaluation considering cost/price and non-cost/price evaluation factors with a focus on adequacy and feasibility.

When the Army received the proposals, the agency first performed a "compliance review." Considering this initial compliance review, the Army eliminated McCann-Erickson USA Inc.'s (ME) proposal from further consideration. Following a debriefing, ME filed an agency-level protest, which was denied. ME then protested to the Government Accountability Office.

ME argued that the Army unreasonably failed to evaluate its proposal meaningfully and instead eliminated ME's proposal from consideration based on a superficial review that only considered whether the firm followed the RFP's proposal preparation instructions. ME asserted that the informational deficiencies in question were minor and could be cured through clarification.

The Army argued that it reasonably eliminated ME's proposal for failing to follow the proposal preparation instructions.

The Comp. Gen. agreed with ME, finding the Army's review to be inconsistent with the solicitation's evaluation criteria. The agency performed a superficial review, and did not meaningfully evaluate the substance of ME's proposal, as required by the solicitation.

The Comp. Gen. noted that the RFP did not advise offerors that the agency would perform a preliminary pass/fail compliance check to determine whether offerors complied strictly with the solicitation's proposal preparation instructions. Agencies must evaluate proposals exclusively based on the solicitation's stated evaluation criteria. While a solicitation may establish additional informational, technical administrative, or other requirements, those requirements may not provide a basis for eliminating a proposal from consideration, unless they are also specified as a basis for proposal evaluation. *Metis Solutions, LLC*, Comp. Gen. Dec. B-411173.2 et al., 2015 CPD ¶ 221, 57 GC ¶ 264; *Veterans Evaluation Servs., Inc., et al.*, Comp. Gen. Dec. B-412940, et al., 2016 CPD ¶ 185.

Though the Comp. Gen. acknowledged that the solicitation included a generic description explaining that award would be made to an offeror who conforms to the solicitation requirements, this language did not appear under the basis of contract award section or the evaluation criteria section.

The Comp. Gen. also found the Army's information concerns were either based on agency errors or related to minor, easily correctible matters.

The first example the Comp. Gen. cited involved the agency's confusion as to the offeror's identity based on the Army's ME proposal review, and the agency's inability to locate ME's representations and certifications in the System for Award Management (SAM) database using the contractor and government entity code that ME provided in its proposal.

The Comp. Gen. found that a fair and comprehensive reading of ME's proposal left no question regarding the offeror's identity, and any questions raised were answered within the proposal. Further, the Comp. Gen. found that ME's representations were indeed complete and accurate on its SAM database profile.

The second example involved Attachment 5—"Preaward Survey of Prospective Contractor Accounting System Checklist," which was to be provided to the Defense Contract Audit Agency for an accuracy review of the offeror's accounting system. ME did not include Attachment 5 in its proposal, and the Army found this to be unacceptable. But ME, which did not have an approved accounting system, followed solicitation instructions and contacted the contracting officer via e-mail to initiate a DCAA accounting-system review. In response to the e-mail, the CO acknowledged that the Army would move forward with the process and there was no further action required from ME at the time. The Comp. Gen. found that the agency unreasonably found the ME proposal unacceptable for not including Attachment 5.

The final example involved the ME cost/price proposal format. ME submitted its cost/price proposal as a portable document file (pdf) rather than a Microsoft Excel spreadsheet. Accordingly, the agency did not conduct a substantive cost/price evaluation, nor did the Army give ME an opportunity to provide the cost/price proposal in an Excel file, or explain why the agency could not evaluate using the pdf version.

The Comp. Gen. found the Army's decision to exclude ME unreasonable. The solicitation evaluation criteria did not provide offerors with notice that proposals would be rejected without a substantive evaluation. Accordingly, the Comp. Gen. sustained the protest.

The Government Contractor Advisory Board

THOMSON REUTERS®

The Government Contractor® (ISSN 0017-2596) is issued weekly, except that no issue is published in the weeks containing January 1, Memorial Day, July 4, Labor Day and December 25, or the week after Thanksgiving ✦ 2017 calendar-year subscription includes annual, accredited "Government Contracts Year In Review Conference" ✦ Attorney Editors: William Schieken, Rick Southern, Ken Berke and Joseph Windsor; Manuscript Editors: Lyrica Johnson and Jennifer LeBerre ✦ Published and copyrighted © 2017 by Thomson Reuters, 610 Opperman Drive, PO Box 64526 St. Paul, MN 55164-0526 ✦ *www.west.thomson.com/dceditorial* ✦ Postage paid at St. Paul, MN. POSTMASTER: Send address changes to The Government Contractor, 610 Opperman Drive, PO Box 64526, St. Paul, MN 55164-0526. For subscription information: call 800.221.9428 or write West, Credit Order Processing, 620 Opperman Drive, PO Box 64833, St. Paul, MN 55164-9753 ✦ All correspondence concerning the content of this publication should be addressed to Thomson Reuters, Attention: The Government Contractor—Editorial Staff, 1333 H. St., NW, Suite 700, Washington, DC 20005.

THE GOVERNMENT CONTRACTOR®

published by Thomson Reuters
610 Opperman Drive
P.O. Box 64526
St. Paul, MN 55164-0526

FIRST CLASS

First Class Mail
U.S. POSTAGE
PAID
Twin Cities, MN
Thomson Reuters

DATED MATERIAL PLEASE DELIVER PROMPTLY

October 2017

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	234	25	26	27	28
29	30	31				

November 2017

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

December 2017

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
$^{24}/_{31}$	25	26	27	28	29	30

Accounting Compliance for Government Contractors
October 23-24
Sterling, VA
$1275

Administration of Government Contracts- A Foundation of Successful Contract Management and Performance
October 17-18
Sterling, VA
$1275

Advanced Issues in Subcontracts and Teaming Agreements
October 17-18
Arlington, VA
$1275

Contract Closeout
October 23-24
Arlington, VA
$1275

Cybersecurity Compliance, Risk Management, and Insurance
October 23
Sterling, VA
$900

DCAA Contractor Business Systems and Internal Controls
October 23-24
Sterling, VA
$1275

Disclosure Statements and Cost Accounting Practices
October 17-18
Sterling, VA
$1275

Federal Grants Compliance
October 23-24
Sterling, VA
$1275

Foreign Corrupt Practices Act (FCPA)
October 23-24
Arlington, VA
$1275

Government Contract Compliance
October 23-24
Sterling, VA
$1275

Government Contract Compliance Week 2017 - DC
October 23-27
Sterling, VA
$2750

Preparing and Defending Government Contract Claims
October 17-18
Arlington, VA
$1275

For full brochures of the above seminars, contact Federal Publications Seminars at 1365 Corporate Center Curve, Suite 101, Eagan, MN 55123 ✦ Phone 888.494.3696 ✦ *www.fedpubseminars.com*