Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Government Contracting's Organic Cybersecurity Evolution

By **Jerald Howe and Kristin Grimes** (August 21, 2019, 6:00 PM EDT)

Jerald Howe

Kristin Grimes

Government contract practitioners find themselves inundated with updates about new and impending cybersecurity regulations. The alphabet soup of references can seem overwhelming at times: DFARS, NIST, FAR, GSAR, FedRAMP, CMMC, etc.[1]

The cast of federal contracting cybersecurity enforcers is also multiplying: undersecretary of defense for acquisition and sustainment, Defense Pricing and Contracting, Defense Contract Management Agency, Defense Industrial Base Cybersecurity Assessment Center, Department of Defense Office of Inspector General, Defense Counterintelligence and Security Agency (formerly the Defense Security Service), Naval Criminal Investigative Service, et al.

Plainly, federal customers — civilian and military — are taking a number of ambitious cybersecurity initiatives. These both "extend" the bar, making cyber requirements apply to more procurements, and "raise" it, by increasing what the government requires to satisfy contractual security requirements.

Meanwhile, in a less noticed development, the fundamental government contracting system is evolving organically to enforce existing cybersecurity requirements. This is especially significant, as until recently, cybersecurity has largely relied upon various forms of "self-attestation."

The acquisition system has seen developments in at least three different areas, each of which will be addressed below: Bid protests, False Claims Act litigation and suspension and debarment. Alexis de Tocqueville wrote that "[t]here is hardly any political question in the United States that sooner or later does not turn into a judicial question." Similarly, just about every new government contracting imperative ends up in each of these arenas. As cybersecurity comes into its own, it is proving to be no exception.

Bid Protests

Governed by the Competition in Contracting Act, Federal Acquisition Regulation Subpart 33.1, and the procedural rules of the U.S. Government Accountability Office and the U.S Court of Federal Claims, the bid protest process is one of the main systemic checks on both would-be contractors and procuring agencies. Given the broad sweep of bid protest jurisdiction over virtually all aspects of proposals and

proposal evaluation, it is natural that such jurisdiction would be exercised over questions of cybersecurity.

With the constantly changing landscape of cybersecurity requirements and guidelines, much is open to a variety of interpretation and debate — creating plenty of opportunities for bid protests. Five such protest decisions represent some of the potential cyber issues in contract award decisions.

Oracle America

This case[2] has received much public attention because it concerns the U.S. Department of Defense's $10 billion, 10-year winner-take-all "JEDI" cloud procurement. Even though it found a deficiency in the DOD's justification for a single award, the U.S. Court of Federal Claims rejected Oracle America Inc.'s protest because it found that Oracle suffered "no prejudice" (and therefore lacked standing to protest).

The JEDI solicitation established several "gate criteria" for an offeror to be included in the competitive range and eligible for award. One of these was "data security" — the relevant evaluation sub-factor required a minimum of three separate cloud data centers, with each support cloud service achieving Federal Risk and Authorization Management Program, or FedRAMP, "moderate" security authorization.

Oracle did not meet this requirement and protested. The court accepted the DOD's argument that this FedRAMP requirement was tied to the "agency's minimum needs" and rejected Oracle's many contentions to the contrary.

This decision should alert companies that new procurements may include tailored and specific cybersecurity criteria that operate to restrict eligibility for award.

Avosys Technology

In this protest,[3] an exclusion based on inadequate past performance was contested. Protestor Avosys Technology Inc. challenged the U.S. Air Force's exclusion of its proposal in an IT services contract competition, which had been based on Avosys' failure to meet past performance evaluation criteria regarding cybersecurity.

Specifically, the Air Force determined that the protestor did not demonstrate it had used solutions to support the data confidentiality and integrity objectives of the risk management framework, a process developed by the National Institute of Standards and Technology, or NIST, that integrates security and risk management activities into the system development life cycle.

The case turned on Section L of the solicitation, which instructed offerors to be clear and specific, and to include sufficient detail for effective evaluation. Given the lack of specific support for offeror's purported cybersecurity capabilities, the GAO found that the agency's evaluation was reasonable.

The key takeaway from this protest decision is that when a request for proposal requires detailed cybersecurity-related past performance, offerors should provide a great level of "clear and specific" detail to demonstrate how they have met stated criteria.

Relying on generalities, invoking boilerplate "industry jargon" and referencing work by subcontractors may be found insufficient to affirmatively demonstrate the merits of an offeror's proposal.

In order to avoid resorting to industry jargon in cybersecurity-related RFPs, prospective contractors would be well advised to engage technical experts with ample lead time.

Another notable aspect here is that the RFP adopted a tiered evaluation process in which offerors had to first meet a capability maturity model integration, or CMMI, Level 2 certification before the agency would evaluate an offeror's technical experience and past performance. This form of "gate criteria" was unchallenged.

The DOD is now working to implement a new Cybersecurity Maturity Model Certification, or CMMC, that draws upon CMMI experience and methods. CMMC will likely be a similar gatekeeper once it goes live on or about June 2020. This case suggests how CMMC may practically operate in future solicitations.

Jardon and Howard Technologies

Rather than contesting its own evaluation, here the protester, Jardon and Howard Technologies Inc., argued that the National Oceanic and Atmospheric Administration should have assigned a deficiency to one of the awardees, Consolidated Safety Services Inc., for failing to adequately address the information technology security requirements in the request for quotations, or RFQ.[4]

CSS' quotation had said it "would provide "[p]rocessing, training, and oversight to meet all SECURITY requirements …" but did not actually use the words "IT Security."

The GAO disagreed and found that the solicitation did not require the level of detail demanded by the protester. In keeping with its general practice, the GAO held that protestor's mere disagreement with the agency's judgment about CSS' failure to satisfy the security requirement was insufficient to overturn the agency's award decision.

Iron Bow Technologies

Vulnerabilities in the supply chain can be the source of weaknesses that potential adversaries can exploit to produce a cybersecurity injury. China has been associated with many instances of "cyberespionage" and therefore is a principal focus of these supply chain risk management, or SCRM, concerns.

In Iron Bow Technologies LLC,[5] the Court of Federal Claims rejected a protest where the U.S. Social Security Administration excluded from award the apparent contract awardee because it was found to present an unacceptable security risk. Iron Bow had proposed to satisfy the solicitation requirements using Lexmark desktop printers.

Pursuant to the RFQ, the government conducted a supply chain risk assessment of the apparent awardee and determined that the potential relationship between Lexmark and the Chinese government justified exclusion of Iron Bow's quotation from consideration.

The court found that the agency's adverse security determination was reasonable and supported by the administrative record. Companies can expect other federal agencies to include solicitation instructions and evaluation provisions tailored to specific security concerns and objectives, and the GAO will generally defer to resulting agency security assessments.

IPKeys Technologies

This somewhat older decision demonstrates that a favorable competitive discriminator may be gained — and sustained if protested — by doing more than what the RFP sets as minimum cybersecurity standards[6] Protestor IPKeys Technologies LLC challenged the Defense Information Systems Agency's, or DISA's, issuance of a task order to By Light Professional IT Services Inc. based on DISA's assessment of a strength under the technical evaluation factor for By Light's cybersecurity approach.

The protestor contended that DISA unreasonably awarded By Light's proposal a strength since the awardee only committed to meeting the RFP's minimum cybersecurity requirements. But DISA responded that the awarded strength was reasonable because By Light's proposal in fact exceeded the RFP's minimum requirements, and that there was no disparate treatment because IPKeys did not commit to implement the heightened cybersecurity procedures as proposed by By Light.

Only By Light had proposed to incorporate the voluntary NIST cybersecurity framework on top of its compliance with the baseline cybersecurity requirements.

The GAO's analysis turned on comparing the RMF and the NIST Cybersecurity Framework. The GAO concluded that the agency reasonably found the two standards to be distinct and complementary.

This decision underscores the need to recognize potentially overlapping sources of cybersecurity best practices and to understand the differences among cybersecurity standards so that proposals can be fashioned to present the strongest achievable credentials to the customer.

Companies may benefit from internal reviews and by measures that produce security credentials beyond the specified minimum. Personnel assigned the duties of proposal writing should be informed of specific security strengths and apply bespoke proposal language rather than "vouching for the minimum" or relying on stock cybersecurity templates that may be adequate but not advantageous in evaluation.

Taken together, these five decisions illustrate, but do not exhaust, the ways in which cybersecurity questions will come to be presented under the bid protest system. All of these protests were denied, in keeping with the general tendency of the COFC and the GAO to defer to agencies, particularly in matters of technical complexity and high stakes security. But as cybersecurity requirements gain in importance in selection processes and decisions, we can eventually expect sustained protests on cybersecurity grounds.

In the bid protest world, the game is never really on until there are sustains in any given area. Only sustained protests will begin to mark the outer limits of how far the COFC or GAO will let agencies roam in exercising their discretion and what agencies must do to document and justify their cyber decisions.

False Claims Act Litigation

The civil False Claims Act is an integral component of the federal contracting system. A civil FCA case can develop with the government itself as a plaintiff, or as a qui tam case, in which a private person — a "relator" or in common parlance, whistleblower — can file suit on behalf of the government.

In a qui tam action, the government investigates and determines whether it will proceed — "intervene" — in the action, though the relator can proceed regardless. While qui tam relators often overreach and

miss the mark, any FCA case that survives an early motion to dismiss results in legal fees, business disruption and financial exposure.

The looming presence of FCA actions already commands attention in diverse areas of cost/pricing, technical/quality and management/compliance areas. Cybersecurity should now be counted among these areas.

Markus v. Aerojet Rocketdyne

An FCA action related to cybersecurity was long predicted, and finally presented in the case of U.S. ex rel Markus v. Aerojet Rocketdyne Holdings Inc. In this case, the relator, Aerojet's former senior director of cybersecurity, compliance and controls, alleged that the company did not satisfy all NIST SP 800-171 security controls as required by the incorporated Defense Federal Acquisition Regulation Supplement, or DFARS, and National Aeronautics and Space Administration FAR Supplement clauses, and under reported the extent of its noncompliance. (The U.S. Department of Justice declined to intervene.)

In May 2019, the U.S. District Court for the Eastern District of California denied, in part, a motion to dismiss the action. The court concluded that the relator plausibly pled that Aerojet's "alleged failure to fully disclose its noncompliance was material to the [g]overnment's decision to enter into and pay on the relevant contracts," as required to establish FCA liability.

The court further ruled that partial disclosures of noncompliance do not relieve liability where there is failure to "disclose noncompliance with material statutory, regulatory, or contractual requirements."[7] The court reasoned that: (1) the government may not have awarded the contracts if it had known the full extent of the company's noncompliance; (2) the area of noncompliance does not need to be the central purpose of the contract, particularly here where cybersecurity compliance could have affected Aerojet's ability to handle technical information relating to missile defense and rocket engine technology and (3) even if the government did not expect full compliance, notice to the government as to the extent of noncompliance must be comprehensive.

Of note, the court further found that the government's decision not to intervene did not impact this determination of materiality.

This case is especially important today to DOD suppliers, at all tiers, as DOD solicitations include DFARS 252.204.7008, which commits all offerors to safeguard covered defense information, or CDI.

As a general FAR rule is being developed to extend cyber protection measures, for all categories of controlled unclassified information, or CUI, to civilian agencies, even more companies are likely to find that a promise to protect CUI is a prerequisite to future federal contracts.

At a minimum, the Aerojet Rocketdyne decision shows that a cybersecurity FCA case — if alleged on the right facts — may be difficult to dispense through preliminary motions practice. This means contractor-defendants will be subjected to extensive discovery and fact finding about their cybersecurity systems, internal evaluations, certifications, etc.

At the same time, former information security insiders who bring cases as qui tam relators will be subjected to discovery and cross-examination into their own actions, motivations, professionalism, etc.

With increasingly complex and stringent cybersecurity requirements, future cases will be more involved.

Once rolled out, the DOD's CMMC may help to mitigate the risks of self-attestation of compliance.

The CMMC regime is expected to provide for a verified third-party's determination of a contractor's cybersecurity "score" which contractors can then rely upon when submitting proposals. Remaining to be addressed is how to deal with degradations or lapses in a contractor's cybersecurity posture after the initial evaluation.

Glenn v. Cisco Systems

Filed in 2011 but kept under seal until settlement and dismissal on July 31, 2019, this case appears to be the first cybersecurity standard-related FCA case with a payout.[8]

The relator was a computer security expert for Danish company NetDesign working on Cisco Systems Inc. products. He claimed that one of these products, Cisco's video surveillance manager, had critical security flaws that violated mandatory cybersecurity requirements for any government computer system, including federal information processing standards, or FIPS, and several NIST SP 800-53 controls.

The relator alleged that Cisco was aware of these flaws since October 2008, but continued to knowingly present claims to the U.S. government for payment or approval while failing to inform government purchasers of critical security flaws or of the VSM's noncompliance with government standards.

Cisco agreed to settle the case for $8.6 million, which includes a partial refund to the U.S. federal government and 16 states for products purchased between 2008 and 2013, as well as approximately $1.6 million to the relator. Cisco's general counsel released a statement acknowledging that while this is a legacy issue and there was no evidence of a breach to any customer's security, standards and expectations are changing and everyone must do more to stay ahead.[9]

The settlement agreement is Cisco's recognition that "what seemed reasonable at one point no longer meets the needs of our stakeholders today." All federal contractors should take heed in this security-focused environment, expecting that more relators — and federal prosecutors — will follow along.

The Cisco settlement also shows that the absence of an actual breach or exfiltration of protected data will not necessarily be a complete defense to a claim for FCA damages.

Suspension and Debarment

The most fearsome weapon in the extensive arsenal of federal contracting enforcement is the government's suspension and debarment power, as set forth in FAR Subpart 9.4. Even a contractor that has been suspended — versus debarred — is dead in the water for future contract awards until the suspension is lifted.

While major contractors are almost never debarred, and rarely suspended for extended time periods, even brief suspensions result in major dislocations, potentially affecting all public sector customers, and bring about extensive negotiations and future compliance commitments in order to lift those suspensions. With the increasing emphasis on cybersecurity requirements, and the perception within parts of the government that contractors have not experienced sufficient adverse consequences to address under-delivery on their security promises, it is unsurprising to see cybersecurity-driven suspension and debarment.

In the recent case of Perceptics LLC, U.S. Customs and Border Protection suspended the Perceptics due to "evidence of conduct indicating a lack of business honesty or integrity" after a hacker attacked Perceptics and posted to the dark web internal CBP traveler data, including faces, license plates, surveillance equipment schematics and sensitive contracting documents.

Perceptics faces administrative proceedings to determine whether it should be debarred. This is one way in which the government can visit severe consequences upon a contractor who experiences a material breach, even if financial or contractual damages are difficult to calculate.

The suspension and debarment system has less public visibility than bid protests or even FCA litigation, so little more is known about the Perceptics situation. Without speculating on specific facts and circumstances, it is nonetheless reasonable to observe that in most cybersecurity incidents, the ultimate outcome depends as much on the timeliness and quality — or lack thereof — of the incident response as on the severity of the underlying breach.

Conclusion

The cybersecurity threat environment will remain very challenging, and virtually everyone agrees that with pending rulemakings and other initiatives underway, cybersecurity requirements in federal contracting will be ratcheted up. As hackers hack, spies spy, regulators regulate and contractors respond, the dynamic will continue to evolve at a rapid pace. Worthy of close attention is how the bid protest, FCA litigation and suspension and debarment systems will fit into this evolutionary process.

Jerald S. Howe Jr. is executive vice-president and general counsel and Kristin Grimes is chief cyber counsel at Leidos Inc.

[1] The referenced regulatory and standards regimes and their acronyms are:

- CMMC — Cybersecurity Maturity Model Certification
- DFARS — Defense Federal Acquisition Regulation Supplement
- FAR — Federal Acquisition Regulation
- FEDRAMP — Federal Risk and Authorization Management Program
- GSAR — General Services Administration Acquisition Regulation
- NIST — National Institute of Standards and Technology

[2] Oracle America Inc. v. United States (COFC) (July 26, 2019)

[3] Avosys Technology Inc. (GAO) (July 30, 2018)

[4] Jardon and Howard Technologies Inc. (GAO) (May 24, 2018)

[5] Iron Bow Technologies LLC vs. United States (COFC) (March 27, 2018)

[6] IPKeys Technologies LLC (GAO) (October 4, 2017)

[7] Citing Universal Health Services Inc. v. United States ex rel. Escobar

[8] U.S. ex rel Glenn vs. Cisco Systems Inc.

[9] https://blogs.cisco.com/news/a-changed-environment-requires-a-changed-approach