Education Alert

Akin Gump
STRAUSS HAUER & FELD LLP

The Beginnings of a Perfect Storm? DOJ's Cyber Review Report, NSPM-33 Research Security Requirements and Aerojet's $9 Million False Claims Act Settlement

August 26, 2022

In July 2022, the Department of Justice (DOJ) released a Comprehensive Cyber Review report (the "Review") summarizing its assessment of its own cyber-related activities and including recommendations focused on its cyber-centric "offensive" (i.e., cyber threat investigations and enforcement) and "defensive" (i.e., approaches to risk mitigation) activities. A key finding declared that "many of the cybersecurity provisions and standards set forth for federal contractors were found to be insufficiently rigorous." The Review went on to note that where contractual cybersecurity standards were not met, the Department's Civil Cyber-Fraud Initiative (CCFI), first announced in October 2021, would continue to utilize the False Claims Act (FCA) to pursue cybersecurity-related cases against government contractors and grant recipients. The Review comes on the heels of a recent FCA settlement with Aerojet Rocketdyne Inc. And, many colleges, universities and independent research institutions are now in the midst of planning for enhanced research security obligations arising out of the January 2022 National Security Presidential Memorandum 33 Implementation Guidance (the "NSPM-33 Guidance").

So what does this mean for the research community?

- DOJ's cyber-fraud initiative should not be ignored. Although the Aerojet case has been pending for several years, it illustrates that the risks of FCA liability in the cyber space are real.
- Careful consideration should be given to the numerous certifications called for by the NSPM-33 Guidance, including a specific certification related to Research Security Program (RSP) requirements. False certifications are a straightforward basis for FCA liability.
- As institutions begin to plan how they will meet the NSPM-33 Guidance's RSP obligations, including the cyber elements, they should recognize that RSP requirements pose more than an administrative compliance risk.

Please reach out to the authors for more information on approaches to managing research security risk.

Michael J. Vernick
Partner
mvernick@akingump.com
Washington, D.C.
+1 202.887.4460

Marta A. Thompson
Counsel
mathompson@akingump.com
Washington, D.C.
+1 202.887.4055

McKenzie F. Miller
Associate
mckenzie.miller@akingump.com
Washington, D.C.
+1 202.887.4517

- While the RSP elements of the NSPM-33 Guidance can seem overwhelming, use of institutional self-assessments and "readiness reviews" can help guide future implementation efforts.

The Aerojet Decision

On July 8, 2022, DOJ announced that Aerojet agreed to pay $9 million to resolve allegations that it violated the FCA by misrepresenting its compliance with cybersecurity requirements in government contracts.[1] Aerojet provides propulsion and power systems for launch vehicles, missiles and satellites, and other space vehicles to the Department of Defense, the National Aeronautics and Space Administration (NASA) and other federal agencies. Those contracts are subject to the Federal Acquisition Regulation (FAR) and agency-specific supplements to the FAR, such as the Defense FAR Supplement (DFARS) and NASA FAR Supplement (NASA FARS), which include provisions requiring compliance with various cybersecurity standards focused on safeguarding information and cyber incident reporting.

The settlement resolves a lawsuit filed by a former Aerojet employee against the company under the *qui tam* or "whistleblower" provisions of the FCA. The whistleblower (or "relator" in FCA parlance), who previously served as the company's senior director of Cyber Security, Compliance & Controls, alleged in the complaint that Aerojet violated the FCA by entering into multiple contracts with federal agencies that required compliance with certain cybersecurity provisions, including those set forth in DFARS 252.704-7012 and NASA FARS 1852.204-76, even though Aerojet knew that its information systems did not meet those standards.

As noted above, the Aerojet case establishes that cyber FCA risk is real, particularly given DOJ's reaffirmation in the Review of its continued willingness to use the FCA as a tool to encourage greater emphasis by the contractor and grantee community on cybersecurity.

The NSPM-33 Guidance's RSP Requirements and FCA Risk

The NSPM-33 Guidance focuses on five discrete areas related to increasing research security: (1) researcher disclosure requirements, (2) use of Digital Persistent Identifiers, (3) consequences for nondisclosure, (4) information sharing within the federal government and (5) RSPs.

The NSPM-33 Guidance requires that institutions that have received more than $50 million in annual science and engineering funding in the previous two fiscal years must establish an RSP. We discussed the elements of an RSP in more detail here, but at a high level the key elements include: (1) a designated research security point of contact, (2) a documented description of the program that must be made available to the government upon request and (3) of particular relevance to this discussion, an institutional certification.

Principal elements of the RSP will focus on foreign travel, research security training, export controls training and cybersecurity. The cyber-specific elements of an RSP include 14 discrete requirements focused on safeguarding information systems. In general, those requirements are similar to the elements of FAR 52.204-21 insofar as they include awareness training, limiting system access to authorized users and authenticating the identities of system users. There are, however, additional research-

focused elements, including an obligation to protect scientific data from ransomware and other data integrity attack mechanisms.

From an FCA risk perspective, the NSPM-33 Guidance explains that once the RSP is in place, institutions will be required to provide a "certification of compliance." Although the language is not yet available, the NSPM-33 Guidance provides that the Office of Science and Technology Policy, National Science and Technology Council, and Office of Management and Budget will work together to develop a standard certification used by all federal agencies. In the coming months, it will be interesting to see how the government utilizes that RSP certification in the grant-making and contract-award processes. For example, will compliance with an RSP be an explicit term and condition of award? While how the RSP will be handled from an award perspective remains to be seen, one can easily imagine FCA cases asserting that an institution falsely certified[2] compliance with its RSP, and by doing so caused the government to award grants and contracts that it would not otherwise have awarded.

Compliance with the cybersecurity elements of an RSP may prove to be a particular challenge for many institutions. Universities, academic medical centers and independent research institutions are often highly decentralized. For example, in the context of a university, the information security systems in the medical school may be distinct from those used by the rest of the campus. Policies may differ, hardware may not be compatible, and/or responsible personnel may report to different elements of leadership, among other issues. In addition, faculty may have servers in their labs, departments may have servers for their own use and various administrative functions may also have dedicated information systems. In short, simply getting one's arms around what constitutes the institution's "information systems" can be extremely difficult. In recent years, as cybersecurity has become more of a front and center risk area, some institutions have moved to place greater control over information security, but those efforts can run afoul of cultures that may frown upon too much central oversight.[3]

As institutions begin to think about how they will develop and implement their RSPs, they will likely grapple with these sort of questions.

So what can research institutions do now?

Recognizing that there is still substantial uncertainty in terms of what the specific RSP requirements will actually look like,[4] what does seem clear is that an institution is quite unlikely to be able to develop and implement an effective RSP without sufficient lead time. In practical terms, planning should start now if it has not already. We have found that some useful tools in the RSP planning process can include self-assessments and what we refer to as "readiness reviews." These activities focus on discrete elements of an effective RSP and seek to understand the current state, the space between where one is today and where one likely needs to be tomorrow, and can help begin framing the discussion around how to get there, taking into account institutional idiosyncrasies and currently available (or obtainable) resources.

[1] The *qui tam case* is *United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al.*, Case No. 2:15-cv-02245-WBS-AC (E.D. Cal.).

[2] The FCA imposes liability on a person who, among other actions, knowingly presents, or causes to be presented, a false or fraudulent claim to the government. 31 U.S.C. § 3729(a)(1). "Knowledge" under the FCA includes actual knowledge, recklessness and deliberate ignorance. 31 U.S.C. § 3730(b).

[3] Although not cyber-related, other elements of the NSPM-33 Guidance pose similar issues. For example, the travel requirements effectively require a degree of insight into faculty and staff travel that may not be currently be available. Obtaining that necessary visibility may be a heavy lift from a culture and resource perspective.

[4] At least on paper, the NSPM-33 Guidance seems to recognize that there will not be a single "one-size-fits-all" solution when it comes to the development and implementation of an effective RSP: "Research organizations should be provided flexibility to structure the organization's research security program to best serve its particular needs, and to leverage existing programs and activities where relevant. . . ." NSPM-33 Guidance at 21. Of course, whether that institutional flexibility is reflected in the actual RSP rollout remains to be seen.

akingump.com