PUBLICATION

DOJ Launches Initiative to Pursue Cybersecurity-Related Fraud by Government Contractors and Grant Recipients

Authors: Erin J. Greten
October 12, 2021

The U.S. Department of Justice (DOJ) recently announced a new Civil Cyber-Fraud Initiative focused on pursuing cybersecurity-related fraud by government contractors and grant recipients. As the federal government focuses attention on federal grantee/subgrantee and subcontractor cybersecurity, it is critical that entities receiving federal funds take prudent action to protect sensitive information and critical systems.

On October 6, 2021, the DOJ announced that its Commercial Litigation Branch, Fraud Section is launching a new initiative to hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. Using the False Claims Act (FCA), the DOJ intends to pursue cybersecurity-related fraud by government contractors and grant recipients. The FCA prohibits and penalizes any individual or entity that "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval" that makes, or causes to be made, false records or statements material to a false claim. (31 U.S.C. 3729, et. Seq.) Specific intent is not required for FCA liability. Contractors/grant recipients/subrecipients may also find themselves in violation of the FCA if they act in deliberate ignorance or in reckless disregard of the truth or falsity of the information. To avoid liability, one must never submit a claim to the federal government that one knows (or should know) is false. This includes incorrectly indicating that one is in compliance with contractual, regulatory, or grant requirements.

Federal Contracts
Federal contracts are governed by the Federal Acquisition Regulations (FAR), and may be required to include clauses such as 52.203-13 requiring internal controls, a written code of business ethics and conduct, due diligence to prevent and detect criminal conduct, the promotion of an organizational culture that encourages ethical conduct and a commitment to compliance with the law, and the disclosure upon creditable evidence that a principal, employee, agent, or subcontractor has committed a violation of federal criminal law or a violation of the FCA. They likely also include the Basic Safeguarding Clause at 52.204-21, but may also contain Department-specific clauses such 252.204-7012 in the Defense FAR. Following President Biden's May 12, 2021 Executive Order on Improving the Nation's Cybersecurity (EO 14028), contractors should be watching for further modifications to the FAR with respect to incident reporting. As of October 4, 2021, an open FAR case is in processing. FAR cases tend to result in new regulations or revisions to existing regulations.

Federal Grants
In the wake of the unprecedented nationwide declaration of emergency issued for the COVID-19 pandemic; many entities have received federal funds for the first time. In addition to specific reporting requirements that may have been imposed by the granting agency, the uniform grant administration regulations at Title 2 of the Code of Federal Regulations (C.F.R.), part 200 contain provisions that could be triggered by a cyber breach or other prohibited action that resulted in a breach.

For example, 2 C.F.R. 200.303 requires that all non-federal entities must establish and maintain effective

internal control over the federal award; must evaluate and monitor the entity's compliance and actually comply with the U.S. Constitution, federal statutes, regulations, and the terms and conditions of the award; must take prompt action when instances of noncompliance are identified, including noncompliance identified in audit findings; and

…take reasonable measures to safeguard protected personally identifiable information and other information the federal awarding agency or pass-through entity designates as sensitive or the non-federal entity considers sensitive consistent with applicable federal, state, local, and tribal laws regarding privacy and responsibility over confidentiality.

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

There is also a mandatory disclosure provision in 2 C.F.R. 200.113 involving all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the federal award as well as 2 C.F.R. Appendix XII requirements (applicable to entities receiving more than $10 million in federal funds) to report certain civil, criminal, or administrative proceedings. Further, related to cybersecurity in general, grant recipients and subrecipients should be aware of 2 C.F.R. 200.216, which prohibits federal grant recipients, subrecipients, and their contractors from using loan or grant funds for certain telecommunications or video surveillance systems. In addition, there may be program-specific requirements related to cybersecurity such as those imposed on financial institutions with respect to federal student financial aid by an institution's Program Participation Agreement with the Department of Education and the Gramm-Leach-Bliley Act (16 C.F.R. 314).

Grant recipients and subrecipients should refer to their award agreements for applicable laws and public policy requirements, such as paragraph XIV of the 2021 Department of Homeland Security Standard Terms and Conditions (applicable to FEMA grants), which requires compliance with the FCA.

For Further Information

If you have questions or need assistance with data protection, privacy, and cybersecurity, including reporting for federal contractors, contact Alisa Chestler or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity team. If you or your entity are being investigated for or need to defend an enforcement action related to a cyber breach, contact Matthew Chester or any member of Baker Donelson's Government Enforcement and Investigations team. For questions regarding requirements for federal contractors, contact Darwin (Skip) Hindman III or any member of Baker Donelson's Government Contracts team. And for questions or assistance with federal grant requirements, particularly disaster assistance grants, including staving off deobligation or clawback, contact Erin Greten or any member of Baker Donelson's Disaster Recovery and Government Services team.