Cybersecurity for government contractors: What you need to know about incident reporting

Stephen Robison | Wednesday, March 23, 2022

Government contracting is one of the best opportunities available to small and medium size businesses. The U.S. government is the largest customer in the world. It purchases everything from office equipment to space rockets. These purchases come in large and small quantities requiring the government to favor small businesses.

Having these contracts can be lucrative to a small business while providing a new level of revenue that might not be possible otherwise. Additionally, these contracts have specific clauses that are found in the Federal Acquisition Regulation (FAR) and include mandates such as requirements concerning cyberattacks and when a business has an obligation to report an incident. These obligations are particularly important when interacting within the national security environment.

Defense contractors must follow the Defense Federal Acquisition Regulation Supplement (DFARS). This document is administered by the Department of Defense (DoD) and supplements the FAR, which is the general guidance the government must follow when purchasing any item. Under the DFARS, requirements are specifically mandated to protect national security and ensure that the entire supply chain is protecting sensitive information. However, this does not mean they only protect secret or top secret information. They also secure the handling of Controlled Unclassified Information (CUI) and Covered Defense Information (CDI). These terms cover information that requires safeguarding but is not classified as a

secret. Under the government definition CUI is considered to be incorporated into 20 Groupings:

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- North Atlantic Treaty Organization (NATO)
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax
- Transportation

Specific CUI categories under these groups can be found in the National Archives.

When individuals think about government contracts, they generally imagine a large business that is producing tanks, airplanes and rockets, or even a construction crew building a new headquarters for an agency. However, to fully understand the extensiveness of different markets to which these laws apply, this post will review the intelligence grouping from above and specifically review the CUI category of Agriculture.

Few people consider farming when they think national security, but under the rules, agriculture is considered CUI. The description provided by the agency defines Agriculture CUI as:

"Information related to the agricultural operation, farming or conservation practices, of the actual land of an agricultural produce or landowner."

Under this rule the Department of Agriculture has determined that it is important to protect the geospatial data concerning specific agricultural land and therefore considers this information to be CUI. Accordingly, if your business then provides any benefit to the supply chain for this agricultural operation and you obtain this specific information you will be required to comply with all federal laws under the FAR and DFARS systems.

Obtaining CUI and/or CDI to fulfill a government contract under the DFARS will also incorporate the National Institute of Standards and Technology (NIST). Applying NIST SP 800-171 requirements to your contracts means you must implement three layers of Incident Response when there is a risk that the information has been stolen, leaked, or breached. Under this rule, if your business possesses any CUI

and/or CDI you will be responsible to:

1. **Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.**
2. **Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.**
3. **Test the organizational incident response capability.**

Therefore, using our example from above, if you were to obtain any of the CUI/CDI concerning the agricultural operation, you will be required by federal law to comply with NIST and implement data privacy and cybersecurity measures.

Overall, a government contract can be a very lucrative line of revenue that can help your business grow and create opportunities for your community. If you are interested in more information concerning the bidding process, our attorneys in the Government Contracting and Procurement Practice Group are available to help. If you are already a government contractor and need help understanding your obligations under the FAR/DFARS/NIST please reach out to our national Data Privacy and Cybersecurity Practice Group, which provides pre-breach services that will ensure you are compliant with all regulations.

Stephen Robison