Articles + Publications | February 13, 2018

New Requirements For Protecting Sensitive Government Data Adopted For Government Contractors: Is Your Company In Compliance?

WRITTEN BY

John S. West | Laura Anne Kuykendall | Michael Gardner

In response to growing cybersecurity threats, the U.S. government has implemented new regulations requiring that its contractors take enhanced measures to protect sensitive government information stored on non-governmental systems and networks, including information stored, accessed, or sent outside the United States. Effective December 31, 2017, government contractors handling sensitive federal government information must comply with cybersecurity requirements found in the Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012, which implements and incorporates the National Institute of Standards and Technology ("NIST") Special Publication 800-171 Revision 1 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations ("NIST SP 800-171 Rev. 1").

Under DFARS regulations, contractors must adhere to two basic cybersecurity requirements: (1) they must provide adequate security to safeguard covered defense information that resides in or transmits through their internal, unclassified systems from any unauthorized access and disclosure; and, (2) they must rapidly report cyber incidents and cooperate with the Department of Defense ("DoD") to respond to these security incidents.[1] In addition, the NIST has imposed particular security controls and requirements with respect to fourteen categories: (1) access controls; (2) awareness and training; (3) audit and accountability; (4) configuration management; (5) identification and multifactor authentication; (6) incident response; (7) maintenance; (8) media protection; (9) personnel security; (10) physical protection; (11) risk assessment; (12) security assessment; (13) systems and communications protection; and, (14) systems and information integrity.[2] Each category contains multiple requirements, resulting in over a hundred different controls. For example, within the access control category, the NIST requires that contractors limit unsuccessful logon attempts and automatically terminate a user session after a defined condition occurs.[3]

Department of Defense contractors who fail to meet these minimum security standards risk losing their DoD contracts. These security controls must be implemented at the contractor and subcontractor levels.[4] Any requests for variances from the requirements established by the NIST must be submitted to DoD's Chief Information Officer ("CIO").[5] For all contracts awarded prior to October 1, 2017, the contractor had an obligation to notify the DoD CIO within 30 days of the contract award of any security requirements specified by NIST SP 800-171 Rev. 1 not implemented at the time of the contract award.[6]

In November 2017, NIST also released draft guidance regarding implementing the NIST's new controls, noting that the guidance was "intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the security requirements".

The Department of Justice's recent Non-Prosecution Agreement with a software development company, Netcracker Technology Corporation, signaled the importance of ensuring that all persons working on government defense and intelligence contracts have appropriate authorization and security clearances. To avoid criminal prosecution, Netcracker agreed to implement an Enhanced Security Plan for its U.S.-based customers' domestic communications infrastructure. Contractors providing goods or services to other private contractors should obtain appropriate assurances regarding the U.S. person status of any person employed or working on behalf of the private contractor and/or the licensed/authorization status applicable under export control laws of foreign persons employed by or working on behalf of the other private contractor. Contractors should take these steps even when supplying DoD or the intelligence community with non-classified commercial off the self ("COTS") products.

Troutman Sanders' Government Contracts and Government Investigations teams have extensive experience in assisting U.S. and non-U.S. clients to ensure that they are in compliance with obligations imposed on government contractors. If you have any questions about the topics discussed in this client alert or if we may assist you in dealing with such matters, please contact Mike Gardner or John West.

---

[1] DFARS 252.204-7012(b), (c).
[2] *See generally* NIST 800-171 Rev. 1.
[3] NIST 800-171 Rev. 1 §§ 3.1.8, 3.1.11.
[4] DFARS 252.204-7012(m).
[5] DFARS 252.204-7012(b)(2)(ii)(B).
[6] DFARS 252.204-7012(b)(2)(ii)(A).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber
- White Collar Litigation + Investigations