CYBERSECURITY LAW ALERT

March 17, 2023

By: Steven J. Kuperschmid, Esq.
Nicole E. Osborne, Esq.
Alexandra C. Piscitello, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Heightened Cybersecurity Standards and Risks: Transacting with the Federal Government

On March 1, 2023, the Biden-Harris Administration released a 35-page National Cybersecurity Strategy ("NCS") which sets out to make fundamental changes to cybersecurity in the United States by investing in certain strategic cyber-related initiatives and rebalancing the responsibility to defend the cyberspace and critical digital infrastructure. The NCS' goal is to expand cybersecurity requirements for government contractors who harbor certain classified and unclassified materials, with the objective of making a national impact.

According to Statista, during the third quarter of 2022, approximately fifteen million data records were exposed worldwide through data breaches. Research indicates that a majority of breaches were attributable to human error. With the tech sector evolving at a rapid pace, the United States' government has vowed to increase efforts to mitigate cyber risks, including via civil penalties for lack of compliance.

The NCS is one part of the Administration's multi-part and ongoing efforts to strengthen America's cybersecurity ecosystem against threats of attack and malicious actors. The federal government has also introduced new laws and initiatives, as well as task forces, including the Justice Department's Cyber-Fraud Task Force to achieve this end.

Impact on Government Contractors and Vendors

According to Strategic Objective 3.5 of the NCS entitled "Leverage Federal Procurement to Improve Accountability," the federal government has found that contracting requirements for vendors that sell to the federal government has proved to be an effective tool for improving cybersecurity as a whole. When a business contracts with the federal government, pursuant to the arrangement the business may be contractually obligated to comply with various cybersecurity obligations. The top four cybersecurity requirements that contracting firms should be aware of are:

(1) The Federal Information Security Modernization Act;

(2) Federal Acquisition Regulation ("FAR") 52.204-21;

(3) DOD Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7012 (mandating compliance with NIST 800-171); and

(4) Cybersecurity Maturity Model Certification 2.0 ("CMMC"). CMMC is currently going through the rulemaking process and federal contractors must stay abreast of future developments.

Risks Associated with Failing to Adhere to the Federal Governments' Cyber Regulations

False Claims Act ("FCA") scrutiny and potentially costly qui tam actions can result from non-compliance with federal cybersecurity requirements. Pursuant to the Civil Cyber-Fraud Initiative, which was introduced in late 2021, the Department of Justice has the power, in accordance with the FCA, to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations. Entities have faced civil actions resulting in monetary penalties, for the following actions, or in certain instances, inactions:

- Knowingly providing deficient cybersecurity which in turn puts information and systems at risk;
- Knowingly misrepresenting cybersecurity practices or protocols; and
- Knowingly violating obligations to monitor and report cyber incidents and breaches.

Given the past success of the federal governments' cybersecurity initiatives aimed at government contractors and the ripple effect that it has on cyber protections for industry in the United States as a whole, as well as the governments' stated initiative in the NCS to "continue pilot[ing] new concepts for setting, enforcing, and testing cybersecurity requirements through procurement," entities who transact with the government can expect heightened cybersecurity requirements from the government in the future.

Additionally, there has been an uptick in civil claims brought against government contractors. For example, certain DoD contractors are required to adhere to NIST 800-171 cybersecurity controls by contract. NIST 800-171 provides recommended requirements for protecting the confidentiality of controlled unclassified information. Defense contractors must implement these recommend requirements (pursuant to contract) to demonstrate they are providing adequate security on IT systems and networks. If federal contractors do not adhere, contracting officers may use available remedies, including withholding progress payments, foregoing remaining contract options, and potentially terminating the contract in part or in whole, to encourage contractors to adhere to policies. The Department of Justice may also institute a FCA litigation if the contractor has attested that they are compliant, when in fact the contractor is not.

This RMF news alert seeks to highlight the key aspects of the NCS initiatives and the cyber regulations that are imposed on federal contractors. If you own or control a business that supplies or otherwise transacts with the federal government, you should familiarize yourself with the requirement specific to your business and make ongoing and regular changes to your company's internal cyber policies. If you have any questions or would like to discuss how this applies to your business, please contact:

Steven J. Kuperschmid, Esq.
516-663-6686
skuperschmid@rmfpc.com

Nicole E. Osborne, Esq.
(516) 663-6687
nosborne@rmfpc.com

Alexandra C. Piscitello, Esq.
516.663.6653
apiscitello@rmfpc.com