PUBLICATION

Cybersecurity a Focus for Biden-Harris Administration in 2022

February 21, 2022

The Biden-Harris Administration made cybersecurity a top priority when President Biden signed Executive Order (EO) 14028 indicating that preventing, detecting, assessing, and remediating cybersecurity incidents in federal government networks would be a focus. Since the signing of EO 14028, the U.S. Department of Justice (DOJ) announced a Cyber-Fraud Initiative, the U.S. Department of Homeland Security formed a Cyber Safety Review Board (CSRB), and the Federal Trade Commission (FTC) announced its intention to seek enforcement actions against organizations that fail to mitigate known cybersecurity vulnerabilities. Since all signs indicate the government will continue its focus on improving cybersecurity related to the services and products provided by government contractors, organizations should prepare for heightened scrutiny from multiple government agencies over their organizational cybersecurity standards and incident responses.

DOJ's Cyber-Fraud Initiative

On October 6, 2021, the DOJ announced its new Civil Cyber-Fraud Initiative team would use the False Claims Act (FCA) to pursue cybersecurity-related fraud by government contractors and grant recipients. The initiative seeks to hold individuals and entities accountable who put U.S. systems and information at risk by:

- Knowingly providing deficient cybersecurity products or services;
- Knowingly misrepresenting their cybersecurity practices and protocols; or
- Knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

As part of this initiative, the DOJ will use the FCA to address government contractors that submit false claims misrepresenting compliance with cybersecurity standards related to information technology, software, cloud-based storage, and other related services.

The FCA provides a remedy of civil damages when a party makes a false statement or engages in a fraudulent course of conduct that is done with knowledge that was material and caused the government to pay out money or forfeit money it was due. A unique aspect of the FCA is it allows private whistleblowers to bring qui tam claims on the government's behalf for which successful whistleblowers stand to receive a bounty of between 15 percent to 30 percent of the total recovery.

The FCA authorizes trebling the actual damages for each false claim in addition to statutory penalties per claim that range from $11,803 to $23,607 (depending on the year when the claim was made). In fiscal year 2021, the DOJ obtained more than $5.6 billion in FCA settlements and judgments. Almost 600 qui tam suits were filed this past year, which yielded $1.6 billion of the year's total FCA recovery.

FTC Warning About Remediating Log4j Security Vulnerability

In response to the discovery of the Log4j software library vulnerability, the FTC sternly warned organizations about their duty to address the vulnerability. It explained that an organization must take reasonable steps to mitigate known software vulnerabilities and violating that duty implicates laws, including the Federal Trade Commission Act and the Gramm Leach Bliley Act. Further, the FTC warned that it will use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data related to the Log4j vulnerability or ***similar known vulnerabilities in the future.***

DHS Cyber Safety Review Board

As directed in EO 14028, DHS established the CSRB on February 3, 2022, and tasked it with reviewing and assessing significant cybersecurity events to protect the nation's networks and infrastructure. The CSRB will be reviewing the Log4j vulnerabilities discovered in late 2021.

Although the announcement clarifies that the CSRB does not have regulatory powers nor is it an enforcement authority, it begs the question as to what extent the CSRB may report findings and concerns to enforcement entities, such as the DOJ. Additionally, monitoring reports issued by the CSRB will likely become an important future consideration for an organization taking reasonable steps to protect consumer data.

Heightened Scrutiny by the Government Requires Increased Planning by Organizations

Since multiple government agencies are focusing on an organization's contractual and regulatory requirements related to cybersecurity, organizations should proactively identify cybersecurity risks and develop a plan to mitigate those risks.

Understanding the cybersecurity requirements in an organization's government contracts is essential to protecting against DOJ enforcement efforts. Expect these contractual requirements to become tighter as the government's focus on improving cybersecurity proceeds. Many government contracts already require contractors to adhere to basic cybersecurity safeguards or attest they fulfill certain cybersecurity standards. Additionally, there may be binding contractual notice requirements for a government contractor. In the past, while non-compliance may have been overlooked, now it could prove costly for an organization under the Biden-Harris Administration's focus on cybersecurity.

An organization's board of directors should increase its oversight over cybersecurity as part of its Caremark duties. Since the issuance of the "Yates Memo," the DOJ has emphasized a need for prosecutors to seek to hold both individuals and organizations accountable. Boards would be wise to consider the following proactive steps in 2022:

- Form cybersecurity subcommittees or create a Cybersecurity Chief Compliance Officer;
- Ask for regular written updates about cybersecurity risks and how the organization is detecting and mitigating those risks;
- Review incident response plans and policies and oversee the updating of any deficiencies; and
- Ensure that there is an internal mechanism for reporting potential cybersecurity non-compliance to decrease the chance of whistleblower claims.

Finally, an organization should consider when to involve outside counsel to preserve certain information under attorney-client privilege. Outside counsel are well suited to assist an organization with both preventive and reactive tasks, which include the following:

- Establishing a timeline of events after an incident;
- Determining post-incident notice requirements and developing a notice playbook;
- Developing cybersecurity compliance procedures and policies;
- Responding to investigatory demands and subpoenas; and
- Meeting and negotiating with government agencies.

The key takeaway here is that the government is signaling it will no longer turn a blind eye to lackluster cybersecurity planning, preparedness, and notice requirements, so organizations should heed that warning and prepare for increased government enforcement efforts.

For more information contact your Baker Donelson Data Protection, Privacy and Cybersecurity attorney.