wiley

ALERT

CISA Publishes Cybersecurity Incident Response and Vulnerability Response Playbooks with Intent of Increasing Expectations for the Private Sector

November 18, 2021

What: On November 16, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released Federal Government Cybersecurity Incident and Vulnerability Playbooks as part of the Biden Administration's efforts to improve the nation's cybersecurity in accordance with Executive Order 14028. The Playbooks are intended to apply to federal civilian executive branch (FCEB) agencies, federal contractors who operate an information system on behalf of a FCEB agency, and information and communications technology (ICT) service providers who have contracted with FECB agencies.

What does it mean for industry: For the private sector, CISA is encouraging all public and private sector partners to review the Playbooks as a way to check their own vulnerability and incident response practices. We encourage organizations to consider how their incident response processes compare to these evolving expectations, as senior government officials have made clear that they expect companies to follow the government's lead in improving cyber readiness.

For additional information about the Playbooks, and how they fit within the Administration's larger approach to cybersecurity for the private sector, continue reading.

**

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Internal Investigations and Compliance Programs

Privacy, Cyber & Data Governance

Securities Enforcement and Litigation

White Collar Defense & Government Investigations

What did CISA do?

CISA issued two different Playbooks to strengthen cybersecurity:

- The Incident Response Playbook applies to incidents that involved confirmed malicious cyber activity and for which a major incident has been declared or not yet reasonably ruled out. Certain federal contractors will be expected to use the Playbook to report cyber incidents. The Playbooks leave the details of such reporting to the specific agencies, stating that, "FCEB ICT Service providers should provide notification of cyber incidents in accordance with FCEB Agency Contracting Officer (CO) requirements." Government service providers should look to their contracts to assess specific reporting requirements and timeframes.
- The Vulnerability Response Playbook applies to any vulnerability that is observed to be used by adversaries to gain unauthorized entry into computing resources. These include known vulnerabilities that have been scored under the Common Vulnerabilities and Exposures (CVE) rating system, as well as unknown zero-day exploits. This Playbook builds on CISA's Binding Operational Directive 22-01 and standardizes the high-level process that FCEB agencies should follow when responding to vulnerabilities that pose significant risk across the federal government, private, and public sectors. The Playbook generally envisions that many vulnerabilities will be patched but also recognizes that other mitigations may be appropriate when patching is not readily possible, stating, "In cases where patches do not exist, have not been tested, or cannot be immediately applied promptly, [agencies should] take other courses of action to prevent exploitation."

Although created to guide federal civilian agencies and covered government contractors, CISA encourages all critical infrastructure entities and private sector organizations to review them "to benchmark their own vulnerability and incident response practices."

The Playbooks are another government "nudge" to private sector standards of care.

The Playbooks have been issued in the midst of an increase in federal government enforcement attention to cybersecurity in the private sector. As Principal Deputy Attorney General (PDAG) John Carlin recently detailed, the U.S. Department of Justice (DOJ) is increasing corporate enforcement actions.

According to Carlin's speech, DOJ will increasingly be using its enforcement initiatives to change corporate behavior so that effective compliance programs are put in place. To do this, DOJ is surging resources for corporate enforcement and is redoubling its commitment to white-collar enforcement. Companies should consider their privacy, national security, cybersecurity, and supply chain programs in light of this warning.

For example, DOJ is increasing its sanctions and export control enforcement, resulting in a substantial increase in open investigations. Around 70% of these cases, PDAG Carlin stated, relate to one of four countries: Iran, the People's Republic of China, Russia, or North Korea. One of the things DOJ is now encouraging is voluntary self-disclosure of potential sanctions or export control violations. Carlin indicated with voluntary disclosure, extensive cooperation, and strong remediation can result in no fine and no monitoring

when the company disgorged the gain that was directly related to its conduct.

All of this follows Deputy Attorney General Lisa O. Monaco's announcement on October 6, 2021, that DOJ is launching a civil cyber fraud initiative to combat new and emerging cyber threats to critical and sensitive information systems. DOJ is putting companies on notice that it will not hesitate to use its civil enforcement authorities to pursue government contractors when they fail to follow required cybersecurity standards. Using the False Claims Act (FCA), DOJ seeks to hold accountable entities or individuals that:

- Knowingly provide deficient cybersecurity products or services;
- Knowingly misrepresent their cybersecurity practices; or,
- Knowingly violate obligations to monitor and report cybersecurity incidents and breaches.

The FCA litigation has already begun to focus on cybersecurity and IT security, and as mandates and certifications multiply, exposure will only increase.

Similarly, the Securities and Exchange Commission (SEC) has been active on cybersecurity. It has repeatedly exhorted its regulated entities about incident reporting and disclosures, to which the CISA Playbooks may be relevant. The SEC has been pursuing formal inquiries into public companies' security incidents and has not been shy about bringing enforcement actions. The SEC recently sanctioned eight firms in three actions for failures in their cybersecurity policies and procedures that resulted in email account takeovers by malicious actors exposing the personal identifying information of thousands of customers and clients at each firm. One firm failed to protect the accounts consistent with their own policies; another failed to adopt firm-wide enhanced security measures for its cloud-based email accounts until three years after it first discovered the email compromise; and, the third company failed to adopt or implement firm-wide security policies until 2020 placing additional customer and client records at risk.

Key Takeaways

Wiley has been advising companies for years to take a risk-management approach to building reasonable cybersecurity programs. In the absence of comprehensive federal law or applicable sector-specific requirements, companies can look to federal contracting standards, the National Institute of Standards and Technology (NIST) publications, industry best practices, and other "soft law" to build effective and defensible programs. Such programs must iterate in response to new threats and the increasing regulatory risk from federal and state government action.

We see substantial and growing regulatory and oversight risk, with new reporting mandates likely in the near future. Federal regulators are leveraging their authorities (and seeking new powers) to demand that companies address threats posed by ransomware, outdated industrial and operational controls, software vulnerabilities, and more.

Companies can help protect against civil fraud enforcement and other litigation and oversight by reviewing relevant cybersecurity requirements and publications like the CISA Playbooks and incorporating government guidance into their own risk management plans. We encourage all organizations to consider how their incident response processes compare to these evolving expectations, as senior government officials have made clear that they expect companies to follow the government's lead in improving cyber readiness.