Published on *The National Law Review* https://natlawreview.com

CISA Issues New Cybersecurity Directive for Federal Agencies

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On November 3, 2021, the Cybersecurity and Infrastructure Security Agency ("CISA") announced Directive 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities (the "Directive"), establishing a CISA-managed catalog of vulnerabilities and compelling federal agencies to remediate such vulnerabilities on government information systems. The Directive targets vulnerabilities that pose a significant risk to the federal government and applies to all software and hardware found on federal information systems, including those managed on an agency's premises, as well as those hosted by third parties on an agency's behalf. The Directive is the latest in a series of executive branch efforts to address U.S. cybersecurity in the public and private sectors.

The Directive requires agencies to take certain steps in connection with remediating the nearly 300 vulnerabilities identified in CISA's catalog; accordingly, agencies must:

- Review and update their internal vulnerability management procedures within 60 days to address, at a minimum, the measures specified in the directive, which include establishing ongoing remediation processes, assigning roles and responsibilities for executing required actions, defining necessary actions to enable prompt responses, establishing internal validation and enforcement procedures for compliance purposes and setting internal tracking and reporting requirements to evaluate and report on compliance, as appropriate. Agencies must provide a copy of their policies and procedures to CISA upon request.

- Remediate each identified vulnerability within the relevant timeframes set forth in the CISA catalog, which range from six months to two weeks. These timeframes are subject to change in light of relevant risks.

- Report on the status of the catalogued vulnerabilities. Agencies are expected to automate data exchanges and report their implementation statuses in accordance with the requirements for deploying the Continuous Diagnostics and Mitigation ("CDM") Federal Dashboard. Agencies that have not migrated reporting to the CDM Federal Dashboard are subject to alternative quarterly reporting, which will entail a bi-weekly requirement beginning October 1, 2022.

CISA provides an option to sign up for automatic alerts when new vulnerabilities are added to the catalog.

As we previously reported, on May 12, 2021, the Biden administration issued an Executive Order on Improving the Nation's Cybersecurity, outlining a number of initiatives intended to improve U.S. cybersecurity and protect federal government networks. Subsequently, the Biden administration has issued orders, directives and guidance on a variety of cybersecurity issues, including those related to requirements for critical pipeline owners and operators, protecting Americans' sensitive data from foreign adversaries, and the development of critical infrastructure performance goals.

National Law Review, Volume XI, Number 313