Lawyer Insights

A Look At Cybersecurity's Federal Legal Landscape

By Adam Solomon and Anna Chan
Published in Law360 | July 26, 2022


This summer, two new U.S. federal laws were enacted to enhance the government's cybersecurity posture at the national, state and local levels.

The new laws — the State and Local Government Cybersecurity Act of 2021, known as the Cybersecurity Act, and the Federal Rotational Cyber Workforce Program Act of 2021, or the Cyber Workforce Program Act — are the latest in a series of executive and legislative actions taken by the federal government over the course of the past year to strengthen cybersecurity resiliency in the U.S.

Following high-profile ransomware attacks on U.S. critical infrastructure, there have been sweeping changes to the federal legal landscape aimed at enhancing cybersecurity defenses and resources in the public and private sectors.

Russia's invasion of Ukraine and the heightened geopolitical tensions have further accelerated these efforts to help the public and private sectors defend against nation-state affiliated attacks.

This recent flurry of cybersecurity-related executive and legislative activity began in May 2021, when President Joe Biden signed Executive Order No. 14028 on improving the nation's cybersecurity.

The executive order sets a number of initiatives intended to bolster cybersecurity capabilities and support of the federal government, such as:

- Establishing a national Cyber Safety Review Board;
- Removing barriers to information sharing between the government and private sector;
- Establishing baseline cybersecurity standards and transparency requirements for software sold to the government; and
- Enabling a governmentwide endpoint detection and response system.[1]

Since the release of the executive order, the administration has issued a number of other orders, directives and guidance on a variety of cybersecurity issues.

Shortly after the executive order was signed, the U.S. Transportation Security Administration issued the first of its four security directives, which impose new cybersecurity standards on certain critical infrastructure operators, such as critical pipelines,[2] passenger railroads and rail transit systems, and

freight railroad carriers.[3]

In June 2021, Biden signed Executive Order No. 14034 on protecting Americans' sensitive data from foreign adversaries, which directed the U.S. Department of Commerce, in coordination with other federal agencies, to monitor software applications that may put the data of Americans at risk, such as applications belonging to companies owned or controlled by foreign adversaries.[4]

The following month, in July 2021, Biden signed a national security memorandum titled "Improving Cybersecurity for Critical Infrastructure Control Systems," which directed the Cybersecurity and Infrastructure Security Agency, or CISA, and the National Institute of Standards and Technology to take the lead in developing cybersecurity performance goals for critical infrastructure sectors.[5]

The CISA, in coordination with the National Institute of Standards and Technology, issued preliminary cross-sector performance goals and objectives in September 2021 to help further a common understanding of the baseline security practices for critical infrastructure.[6]

In March, the U.S. Senate unanimously passed the Strengthen American Cybersecurity Act of 2022, which was comprised of three bills:

1. The Federal Information Security Modernization Act;

2. The Cyber Incident Reporting for Critical Infrastructure Act, or CIRCIA; and

3. The Federal Secure Cloud Improvement and Jobs Act.

This new version of the Federal Information Security Modernization Act would continue the government's efforts in modernizing its cybersecurity resilience and allow for better coordination and communication between federal agencies with respect to information security management, while the Federal Secure Cloud Improvement and Jobs Act would streamline the process in which federal agencies can receive approval for cloud technologies.[7]

The U.S. House of Representatives packaged the CIRCIA as part of an omnibus spending bill, which was subsequently passed and enacted into law that same month.[8]

Under the CIRCIA, covered critical infrastructure entities must notify the CISA within 72 hours of discovering a covered cyber incident and within 24 hours of a ransomware payment.[9]

The CIRCIA is expected to have far-reaching implications for a broad range of businesses, including those in the energy, financial services, commercial facilities, communications, information technology, transportation systems, health care and public health.

Most recently, in June, two additional cybersecurity bills, the previously mentioned Cybersecurity Act and the Cyber Workforce Program Act, were enacted into law. Both of these laws align with the recent efforts by the federal government to enhance U.S. cybersecurity.

The Cybersecurity Act aims to improve coordination between the U.S. Department of Homeland Security's CISA and state, local, tribal and territorial governments, as well as corporations, associations and the general public.

A Look At Cybersecurity's Federal Legal Landscape
By Adam Solomon and Anna Chan
Published in Law360 | July 26, 2022

The Cybersecurity Act imposes a number of obligations upon DHS, such as DHS' National Cybersecurity and Communications Integration Center, to allow for better collaboration between federal and nonfederal entities.

Such collaborations, upon the requests of state, local, tribal and territorial governments, include:

- Conducting cyber-preparedness exercises;
- Providing operational and technical training;
- Promoting cybersecurity education and awareness;
- Sharing of certain information in real time, e.g., cyber threat indicators, defensive measures and information about incidents; and
- Providing notifications containing specific incident and malware information that may affect such local governments or their residents.[10]

The Cyber Workforce Program Act establishes a rotational workforce development program, which would allow federal cybersecurity professionals to rotate through multiple federal agencies.[11]

This program is intended to enable cybersecurity professionals to more easily boost their expertise by rotating through agencies to gain new skills and experience, which may allow the federal government to more easily compete with the private sector in terms of attracting and recruiting top talent.

Building on the momentum of the recent legislative and executive initiatives, additional efforts to improve the nation's cybersecurity defenses are expected.

To date, a number of cybersecurity bills are currently pending in Congress as well as numerous state legislatures.

Based on the legislative and executive actions taken so far, legislators and regulators appear to be increasingly focused on improving cyber preparedness, enhancing threat monitoring and incident response capabilities, and promoting more coordination among governmental and nongovernmental entities.

Whether in the public or private sector, organizations should take these efforts into consideration when developing their own cybersecurity programs.

A Look At Cybersecurity's Federal Legal Landscape
By Adam Solomon and Anna Chan
Published in Law360 | July 26, 2022

Notes

1.The White House, Executive Order on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last visited July 2022).

2. Press Release, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators (last visited July 2022).

3. Press Release, DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (December 2, 2021), https://www.tsa.gov/news/press/releases/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation (last visited July 2022).

4. The White House, Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries (June 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/ (last visited July 2022).

5. The White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (last visited July 2022).

6. CISA, Cross-Sector Cybersecurity Performance Goals and Objectives (September 22, 2021), https://www.cisa.gov/cpgs (last visited July 2022).

7. Strengthen American Cybersecurity Act of 2022, S.3600, available at https://www.congress.gov/bill/117th-congress/senate-bill/3600/text (last visited July 2022).

8.Consolidated Appropriations Act 2022, Pub. L. No. 117-103, H.R. 2471, 117th Cong., 990-1011 (2022).

9. Id. at 994-1001.

10. State and Local Government Cybersecurity Act of 2021, S.2520, available at https://www.congress.gov/bill/117th-congress/senate-bill/2520/text (last visited July 2022).

11. Federal Rotational Cyber Workforce Program Act of 2021, S.1097, available at https://www.congress.gov/bill/117th-congress/senate-bill/1097/text (last visited July 2022).

A Look At Cybersecurity's Federal Legal Landscape
By Adam Solomon and Anna Chan
Published in Law360 | July 26, 2022

Adam Solomon *is a counsel in the firm's global privacy and cybersecurity practice in the firm's New York office. Adam assists clients in identifying, evaluating and managing global privacy and information security risks and compliance issues. He can be reached at +1 (212) 309-1327 or asolomon@HuntonAK.com.*

Anna Chan *is a counsel in the firm's global privacy and cybersecurity practice in the firm's New York office. Anna assists clients in identifying, evaluating, and managing privacy and information security risks and advises clients on federal, state, and international privacy obligations. She can be reached at +1 (212) 309-1194 or achan@HuntonAK.com.*