GIBSON DUNN

President Biden Issues Executive Order to Enhance U.S. Cybersecurity in the Wake of Major Cyber Incidents

Client Alert | May 18, 2021

Related People

Eric D. Vandevelde

Ryan T. Bergsieker

Lindsay M. Paulin

Jennifer Katz

Terry Wong

I. Introduction

Following two major cybersecurity events, President Biden issued a sweeping Executive Order on May 12, 2021,[1] reinforcing his commitment that fighting cyberattacks is "a top priority and essential to national and economic security." The executive action is the latest of the Administration's efforts on "prevention, detection, assessment, and remediation of cyber incidents," coming on the heels of the Colonial Pipeline ransomware attack, and just a few months after the SolarWinds breach.

In brief, reports in December 2020 revealed that hackers accessed the systems of SolarWinds, an IT management software company, and implemented malicious code that enabled the hackers to install malware that was used to spy on SolarWinds and its customers, including several U.S. government agencies and many Fortune 500 companies. And in early May 2021, Colonial Pipeline, an oil pipeline system, was targeted by a criminal cybergroup encrypting its system and demanding a ransom. Although aimed at business technology, the attack caused Colonial Pipeline to shut down operations on a major pipeline serving the Northeast, leading to gas shortages and panic buying.

These two high-profile incidents illustrate the reality that cyberattacks are a growing threat facing both the public and private sectors. The scope and incidence of these attacks has grown steadily year over year, with experts from Cybersecurity Ventures estimating that cybercrime will cost $6 trillion globally in 2021 and continue to grow by 15% annually over the next five years.[2] Cyberattacks can have wide-ranging implications, including theft of sensitive personal data, breach of state and trade secrets, and network and power disruptions, so investment in cybersecurity infrastructure is critical.

In light of these threats, the Order is the latest step in the Biden Administration's commitment to "disrupt and deter our adversaries from undertaking significant cyberattacks." President Biden's appointments have signaled his seriousness in this regard — he has appointed a number of experienced cybersecurity professionals to significant roles, including for the newly-created role of National Cyber Director and a Deputy National Security Advisor for Cyber and Emerging Technology (a role that elevated the subject within the Administration). While the Administration has indicated intentions to push for more comprehensive cybersecurity legislation, in the interim, the Order will have a significant impact on the way that federal government agencies and government contractors approach cybersecurity. The Administration intends the Order to also "encourage private sector companies to follow the Federal Government's lead," a strategy that had prior success with the widespread adoption of the National Institute of Standards and Technology's 2014 voluntary cybersecurity framework.

II. Key Provisions of the Executive Order

The Order aims to improve the nation's cybersecurity and protect federal government networks against sophisticated, malicious cyber activity from both nation-state actors and cyber criminals. As many high-profile cyber incidents have shared risk factors and other commonalities, such as similar cybersecurity vulnerabilities and a lack of robust defenses, the Order focuses on measures likely to have an immediate and wide-ranging impact on critical infrastructure systems, such as strengthening federal network protections, promoting information-sharing between the U.S. government and private sector, and enhancing the ability to respond to incidents. While many federal agencies and contractors already maintain and abide by existing agency-specific cybersecurity measures, the Order establishes additional mechanisms and standards to ensure that all information systems used or operated by federal agencies or contractors "meet or exceed" the cybersecurity standards and requirements set forth in the Order.

The Order aims to spur substantial participation and investment from a diverse array of relevant stakeholders in both the public and private sectors. Although the Order's requirements apply only to federal agencies and contractors, the Order acknowledges the private sector's integral role in providing and maintaining domestic critical infrastructure. To this end, the Order expressly encourages the private sector — including entities that are not government contractors — to adopt comparable and ambitious measures to minimize future cyber incidents.

The Order contains eight key components and provisions for modernizing the federal government's defenses and responses to cyberattacks, which are summarized below.

Sec. 2. Removing Barriers to Sharing Threat Information.

The Order calls for the review and update of Federal Acquisition Regulation ("FAR") and Defense Federal Acquisition Regulation Supplement ("DFARS") requirements to ensure that federal contractors collect, preserve, and share information related to cyber threats and incidents. The anticipated revisions to the FAR and DFARS provisions would also require service providers to collaborate with federal agencies in investigating and responding to incidents or potential incidents. The Order establishes a federal government policy that information and communications technology service providers must promptly report the discovery of cyber incidents to the appropriate federal agencies, and contemplates revisions to the FAR identifying the types of cyber incidents that will trigger such reporting, the types of information to be reported, the time periods within which to report cyber incidents based on a graduated scale of severity, and the types of contractors and service providers to be covered by the proposed language. The Order also contemplates the standardization of agency-specific cybersecurity requirements through the anticipated FAR updates. Furthermore, the Biden Administration has conveyed its expectation that these revised contract terms will spur adoption of the practices by the private sector more broadly.

Sec. 3. Modernizing Federal Government Cybersecurity.

Recognizing that the cyber threat environment is "dynamic and increasingly sophisticated," the Order identifies necessary steps for modernizing its approach to cybersecurity and ensuring effective defenses, including: (1) adopting security best practices; (2) advancing toward Zero Trust Architecture; (3) accelerating movement to

secure cloud services, including Software as a Service (“SaaS”), Infrastructure as a Service (“IaaS”), and Platform as a Service (“PaaS”); (4) centralizing and streamlining access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and (5) investing in both technology and personnel to match these modernization goals.

Tools such as multi-factor authentication and encryption for data at rest and in transit, as well as endpoint detection response, logging, and operating in a zero-trust environment, will be rolled out across federal government networks on a tight timeline. The Order also requires the development of cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection, as well as the development and issuance of a cloud-service governance framework. Notably, the Order also requires modernization of the existing FedRAMP program, a government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring of cloud products and services.

Sec. 4. Enhancing Software Supply Chain Security.

The Order also seeks to improve the security of commercial software used by the federal government in three ways. First, the Order calls for the creation of baseline guidelines and standards for the security of software used by the federal government based on industry best practices established by the National Institute of Standards and Technology (“NIST”) with input from “the Federal Government, private sector, academia, and other appropriate actors.” Second, the Order seeks to jumpstart the market for secure software by leveraging federal buying power. The Order requires the FAR Council to consider recommendations for contract language requiring software suppliers to comply with, and attest to complying with, the new software standards. Agencies will then be directed to remove and remediate software products that do not meet the amended FAR requirements. Third, the Order directs NIST to develop a cybersecurity “pilot program” labeling initiative to give consumers visibility into the security of the software.

Sec. 5. Establishing a Cyber Safety Review Board.

The Order establishes a Cyber Safety Review Board composed of both federal officials and representatives from private-sector entities to review and assess threat activity, vulnerabilities, mitigation activities, and agency responses related to “significant” cyber incidents. The Board, which is modeled after the National Transportation Safety Board’s investigations of civil transportation incidents, would convene following significant cyber incidents and provide recommendations for improving cybersecurity and incident response practices.

Sec. 6. Standardizing the Federal Government’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.

As current cybersecurity vulnerability and incident response procedures vary across agencies, the Order calls for standardized response processes to “ensure a more coordinated and centralized cataloging of incidents and tracking of agencies’ progress toward successful responses.” The Order mandates that federal agencies work together in the development of a “standard set of operational procedures (playbook)” that incorporates NIST standards, as well as articulates all phases of an incident response while also building in flexibility. The Administration intends for this playbook to “also provide the private sector with a template for its response efforts.”

Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks.

Endpoint detection and response is an emerging technology intended to address the need

for continuous monitoring and response to advanced threats. The Order calls for an Endpoint Detection and Response (EDR) initiative to "support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response." Federal adoption of EDR has lagged behind the private sector, which has already begun incorporating it as central component of cybersecurity programs within industry.

Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities.

The Order requires "agencies to establish requirements for logging, log retention, and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency," and requires that the FAR Council consider the recommendations for these policies in promulgating the revisions to the FAR described in Section 2 of the Order. Therefore, companies should anticipate changes to contractual requirements to establish logging policies.

Sec. 9. National Security Systems.

The Order calls for "National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order that are otherwise not applicable to National Security Systems," which will be reflected in a National Security Memorandum ("NSM"). Generally speaking, a "national security system" is an information system used or operated by an agency or contractor that involves intelligence activities, cryptologic activities, command and control of military forces, equipment integral to a weapon or weapons system, or that is critical to the fulfilment of military or intelligence missions.

III. Analysis and Takeaways

Among the many takeaways from the Order, the most noteworthy is the expected and intended impact beyond federal agencies and contractors, given the express goal of influencing the broader private sector's cybersecurity best practices. The Order's ultimate impact will largely be shaped by the regulations issued in the coming months to comply with these new requirements.

- The Order contemplates an aggressive timeline for these reforms, with deadlines ranging between 45 and 120 days for agencies to begin implementing many of the Order's key requirements.
- Many of these requirements have already been established as common or best practices in the private sector, but widespread adoption by federal agencies may encourage additional private sector businesses to conform to these standards.
- With the forthcoming guidelines, private companies — regardless of whether they intend to pursue federal contracts — may see a new "best practice" to which its own standards will be compared and evaluated. As a result, the requirements promulgated in response to the Order could impact what amounts to "reasonableness" and the duty of care for civil liability.
- The Order's recognition of the need for collaboration and cooperation between the federal government and the private sector creates an opportunity for input from private sector stakeholders. Industry should monitor forthcoming rulemakings to

implement the Order and consider opportunities to comment.

The legal issues and obligations related to Executive Order 14028, entitled “Improving the Nation’s Cybersecurity,” are likely to shift as federal agencies implement its provisions. We will continue to monitor and advise on developments to stay on the forefront of this rapidly-changing area. We are available to guide companies through these and related issues. Please do not hesitate to contact us with any questions.

---

[1] *See* Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021).

[2] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Cybercrime Magazine (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.

This alert was prepared by Alexander H. Southwell, Eric D. Vandevelde, Ryan T. Bergsieker, Lindsay M. Paulin, Jennifer Katz and Terry Y. Wong.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work in the firm’s Privacy, Cybersecurity and Data Innovation or Government Contracts practice groups, or the following authors:

Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Lindsay M. Paulin – Washington, D.C. (+1 202-887-3701, lpaulin@gibsondunn.com)
Jennifer Katz – New York (+1 212-351-4066, jkatz@gibsondunn.com)

Privacy, Cybersecurity and Data Innovation Group:

United States
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Government Contracts Group:
Dhananjay S. Manthripragada – Los Angeles (+1 213-229-7366, dmanthripragada@gibsondunn.com)
John W.F. Chesley – Washington, D.C. (+1 202-887-3788, jchesley@gibsondunn.com)
Joseph D. West – Washington, D.C. (+1 202-955-8658, jwest@gibsondunn.com)
Lindsay M. Paulin – Washington, D.C. (+1 202-887-3701, lpaulin@gibsondunn.com)
Justin Paul Accomando – Washington, D.C. (+1 202-887-3796, jaccomando@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation