President Biden issues broad-ranging Executive Order on cybersecurity

Cybersecurity Law Alert

13 May 2021
By: Lea Lurquin | Jeff DeGroot | Andrew Serwin

Yesterday, in the wake of several high-profile cybersecurity incidents, President Biden issued an Executive Order on Improving the Nation's Cybersecurity. The Order, which acknowledges the "increasingly sophisticated malicious cyber campaigns that threaten the public [and] private sector," sets forth new requirements for federal agencies and government service providers.

Specifically, the Order addresses:

- **Updating government contracts to remove barriers to sharing threat information**: The Order mandates that contracts with information technology and operational technology service providers be updated to require these service providers to preserve information relevant to cyber incidents and share information with appropriate agencies. The Order further specifies that contracts with information and communications technology service providers contain cyber incident reporting obligations and that all agency contracts have standardized cybersecurity requirements. These changes stem from "current contract terms or restrictions [imposed on government service providers that] may limit the sharing of … threat or incident information with executive departments and agencies … that are responsible for investigating … cyber incidents."
- **Modernizing federal government cybersecurity**: The Order directs federal agencies to review and update their cybersecurity capabilities by, among other things, implementing Zero Trust Architecture, adopting multi-factor

authentication, and encrypting data in transit and at rest. Zero Trust Architecture refers to security programs that assume threats are inside and outside of their controlled network(s), requiring additional access controls that detect threats that may come from shared users of a particular platform or service. The Order additionally seeks to modernize FedRAMP by establishing training programs for agencies and streamlining documentation that vendors are required to complete.

- **Enhancing software supply chain security**: Starting with the premise that "[t]he development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors," the Order sets forth steps designed to improve software security:
  - First, the Order calls for guidance – created through input from the federal government, the private sector, and academia – to enhance the security of the software supply chain, which will include standards for secure software development.
  - Second, the Order mandates identification of "critical software" – for example, software affording or requiring elevated system privileges or direct access to networking and computing resources – that federal agencies use and guidance outlining security measures for critical software.
  - Third, the Order initiates a pilot consumer-labeling program aimed at educating the public on the security capabilities of Internet-of-Things devices and software development practices.

- **Creating a new Cyber Safety Review Board**: The Order creates the Cyber Safety Review Board – a board modeled after the National Transportation Safety Board – which will review and assess significant cyber incidents and, based on its review, provide recommendations for improving incident response practices.
- **Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents**: To address the issue of varying incident-response procedures among agencies, the Order mandates the development of "a standard set of operational procedures (playbook) to be used [by federal agencies] in planning and conducting a cybersecurity vulnerability and incident response activity …."
- **Improving detection of cybersecurity vulnerabilities and incidents on federal government networks**: The Order mandates that federal agencies "deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure" in order to "maximize the early detection of cybersecurity vulnerabilities and incidents on [their] networks."
- **Improving the federal government's investigative and remediation capabilities** : To help address cyber incidents on federal agency systems, the Order calls for the creation of new policies to address logging, log retention, and log management.

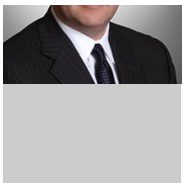
DLA Piper's Data Protection, Privacy and Security practice will continue to track developments as the federal government creates specific mandates for agencies and private companies pursuant to this Order. Learn more about the implications of the EO by contacting us via PrivacyGroup@dlapiper.com.

AUTHORS

Lea Lurquin
Associate
San Francisco | T: +1 415 836 2500
lea.lurquin@dlapiper.com

Jeff DeGroot
Associate
Seattle | T: +1 206 839 4800
jeff.degroot@dlapiper.com

Andrew Serwin
Partner
San Diego (Golden Triangle) | T: +1 858 677 1400



andrew.serwin@dlapiper.com