BLANKROME
CELEBRATING 75 YEARS

Privacy, Security & Data Protection and Government Contracts

MAY 2021 • NO. 1

President Biden's Recent Cybersecurity Executive Order Will Increase Compliance Obligations on the Private Sector

Companies providing information technology products and services to U.S. government agencies are now required to notify such agencies of cyber incidents and meet specific cybersecurity standards. The executive order attempts to modernize the federal government's cybersecurity defenses by "protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the [United States]' ability to respond to incidents when they occur." The executive order is just one example of the Biden administration's push to improve the nation's data privacy and cybersecurity practices in response to the recent series of ransomware attacks.

On May 12, 2021, President Biden signed an executive order to bolster the federal government's cybersecurity practices and contractually obligate the private sector to align with such enhanced security practices ("the Order"). The Order comes on the heels of a ransomware attack on Colonial Pipeline that occurred on May 6, 2021, which shut down the largest oil pipeline in the United States and disrupted supplies of gasoline, diesel, and jet fuel to the East Coast. This initiative to improve the security of the software supply chain also stems from the SolarWinds cyberattack that occurred last year. In the attack, Russian hackers used a routine software update that Texas-based SolarWinds Corp. provided to its customers to install malicious code, allowing the hackers to infiltrate nine federal agencies and about 100 companies.

Proposed amendments are expected soon from the Federal Acquisition Regulation ("FAR") and the Defense Federal Acquisition Regulation Supplement ("DFARS") that will increase compliance obligations for government contractors and their vendors, building on a string of supply chain and cybersecurity regulation in recent years (including Section 889's prohibition on the use of certain Chinese telecommunications, new registration requirements in the Supplier Performance Risk System, and the Department of Defense's Cybersecurity Maturity Model Certification program). We see the biggest impacts on government contractors, such as developers and users of software.

The Order:

- **Removes Barriers to Threat Information Sharing between the Government and the Private Sector.** The Order removes certain contractual barriers that prevent information technology ("IT") service providers from sharing information about cyber incidents with government agencies with which they contract and requires the IT service providers to promptly notify such agencies of a cyber incident involving the software and support-related

products or services they provide. The Order requires the FAR Council to update the FAR and the DFARS to remove the contractual impediments to sharing information about cyber incidents and to detail the information that must be included in a cyber incident notification to government agencies, including the time periods for reporting cyber incidents (a three-day deadline for the most severe incidents). The Order also requires IT service providers to cooperate with federal agencies to investigate and respond to incidents on federal information systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with government agencies. Department of Defense contractors are already subject to similar cyber reporting and cooperation requirements. This means that the Order will have the greatest impact on civilian agency contractors, which, to date, have generally not been required to report cyber incidents to the U.S. government.

- **Modernizes and Implements Stronger Cybersecurity Standards in the Federal Government.** The Order mandates government agencies to move to secure cloud services and a zero-trust architecture. The Order further mandates deployment of multifactor authentication and encryption for data at rest and in transit within 180 days of the date of the Order.

- **Improves Software Supply Chain Security.** The Order requires all software purchased by the federal government to meet, within six months of the Order, a series of new baseline security standards, which includes requiring developers to maintain greater visibility into their software and making security data publicly available. The Order seeks to amend the FAR/DFAR to include language requiring government software suppliers to attest to complying with the new security standards. The Order also establishes a pilot program to create an "energy star" type of label so the government and the public at large can quickly determine whether software was developed securely. The Order directs the Secretary of Commerce, through the National Institute of Standards and Technology ("NIST"), to consult with federal agencies, the private sector, academia, and other stakeholders in identifying standards, tools, best practices, and other guidelines to enhance software supply chain security. NIST recently announced it will host a virtual workshop on June 2 and 3, 2021, to share NIST's plans to develop software-related standards and guidelines called for by the Order, and receive and discuss information and ideas about the approach and content that NIST should consider in developing those standards and guidelines.

- **Establishes Cybersecurity Safety Review Board.** The Order establishes a Cybersecurity Safety Review Board, comprised of government and private-sector officials to review and assess major cyber incidents and make concrete recommendations for improving cybersecurity. The first incident to be reviewed by the Cybersecurity Safety Review Board is the SolarWinds attack.

- **Creates Standard Playbook for Responding to Cyber Incidents.** The Order creates a standardized playbook and set of definitions for cyber incident response by federal departments and agencies that incorporate NIST standards. The playbook will also provide the private sector with a template for its response efforts.

- **Improves Detection of Cybersecurity Incidents on Federal Government Networks.** The Order improves the ability to detect malicious cyber activity on federal networks by requiring initiatives to identify deployment options for a government-wide endpoint detection and response system, and enabling improved information sharing within the federal government.

- **Improve Investigative and Remediation Capabilities.** The Order creates cybersecurity event log requirements for federal departments and agencies.

To address weaknesses in national cyber defense that have been recently exposed with the SolarWinds hack and the recent series of ransomware attacks, including on Colonial Pipeline, the Order seeks to "improve the nation's cybersecurity and protect federal government networks" and address the "insufficient cybersecurity defenses that leave public and private sector entities more vulnerable to [cyber] incidents." The rise of ransomware attacks in the United States has also caused the Department of Justice ("DOJ") to create a new task force to unify efforts across the federal government to pursue and disrupt ransomware attackers. Moreover, the U.S. government has signaled that cybersecurity will be a critical factor when evaluating contractors for new contracts. Contractors who can demonstrate compliance with the Order and other new cybersecurity initiatives will be more competitive than their non-compliant counterparts.

In addition to the Order, the Biden administration will likely continue to focus its attention on cybersecurity. Since his campaign, President Biden has stated that he would prioritize data privacy and security on his agenda. Consistent with that statement, President Biden selected veteran cybersecurity leaders to be part of his administration, including former National Security Agency official Jen Easterly to serve as Director of Cybersecurity & Infrastructure Security Agency, former California Attorney General Xavier Becerra (who enforced the California Consumer Privacy Act during his time as Attorney General) to serve as the Secretary for Health & Human Services and former Department of Homeland Security senior official Alejandro Mayorkas (who has addressed diverse cyber threats and negotiated a key cybersecurity agreement with China) to serve as Homeland Security Secretary. These officials are in good company with Vice President Kamala Harris, who during her career as California Attorney General issued privacy recommendations for mobile devices, published a joint statement with tech giants on privacy principles to be followed for mobile platforms and created the Privacy Enforcement and Protection Unit of the California Attorney General's Office to enforce privacy and data breach notification laws. Additionally, earlier this year, President Biden announced, and Congress passed, the American Rescue Plan Act, which appropriates $650 million to the Cybersecurity and Infrastructure Security Agency ("CISA") to conduct cyber risk mitigation efforts, $1 billion to the General Services Administration's ("GSA") Technology Modernization Fund, and $200 million for the United States Digital Service.

With the Biden administration's push toward strengthening data privacy and cybersecurity, companies that do business with the U.S. government should closely monitor all developments in the federal landscape. This includes all developments related to the Order, any guidance provided by the DOJ's new task force, and possibly the passage of a comprehensive federal privacy law. Contractors should also make sure that they comply with existing cybersecurity requirements, such as the Cybersecurity Maturity Model Certification program, registration in the Supplier Performance Risk System, and compliance with applicable NIST standards. The U.S. government will strengthen its cybersecurity posture by building on these existing programs, making it important that contractors are already in compliance with existing requirements.

We will continue to monitor and report on the recommendations and amendments to the FAR and DFARS that are to come under the Order in the near future.

For additional information, please contact:

PRIVACY, SECURITY & DATA PROTECTION

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Alex C. Nisenbaum
949.812.6011 | alex.nisenbaum@blankrome.com

Karen H. Shin
949.812.6012 | karen.shin@blankrome.com

GOVERNMENT CONTRACTS

Justin A. Chiarodo
202.420.2706 | jchiarodo@blankrome.com

Michael J. Montalbano
215.569.5618 | mmontalbano@blankrome.com