King & Spalding
Client Alert

Government Matters

MAY 18, 2021

For more information, contact:

Steve Cave
+1 202 215 8506
scave@kslaw.com

Rick Vacura
+1 703 245 1018
rvacura@kslaw.com

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Mark Villapando
+1 703 245 1023
mvillapando@kslaw.com

King & Spalding

Northern Virginia
1650 Tysons Blvd
Suite 400
McLean, VA 22102
Tel: +1 703 245 1000

Washington, D.C.
1700 Pennsylvania Ave., NW
Washington, D.C. 20006
Tel: +1 202 737 0500

President Biden's Executive Order to Improve Cybersecurity Issued

On May 12, 2021, President Joe Biden issued a wide ranging Executive Order "On Improving the Nation's Cybersecurity," which was in the works after the SolarWinds cyberattack and arrived soon after a ransomware attack on the Colonial Pipeline Company that cut off fuel supply to most of the east coast of the United States. The Order places responsibility on both the Departments of Defense and Homeland Security to require agencies to protect their data, provide for more information sharing of cyber-attacks, and establishes a cyber incident review group. The Order includes the following information and procedures relevant to all federal government contractors and subcontractors.

SHARING THREAT INFORMATION

The Order recognizes that contracts with information and operational technology providers may include terms and conditions that limit the sharing of threat or incident information to agencies that investigate cyberattacks. The Order also recognizes that cybersecurity requirements in unclassified contracts vary among agencies. Accordingly, the Director of the Office of Management and Budget (OMB) must consult with the Secretaries of Defense and Homeland Security, Attorney General, and Director of National Intelligence to review and recommend updates to the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement so that service providers may share data with those agencies consistent with applicable privacy laws, and use standard contract language for appropriate cybersecurity requirements.

MODERNIZING FEDERAL GOVERNMENT CYBERSECURITY

The Director of the Cybersecurity and Infrastructure Security Agency (CISA), along with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP), will develop and implement security principles as agencies move toward using cloud service providers that include Software as a Service, Infrastructure as a Service, and Platform as a Service. The Order requires all agencies to implement security measures using multi-factor authentication and data encryption as they move towards Zero Trust Architecture.

ENHANCING SOFTWARE SUPPLY CHAIN SECURITY

The Director of the National Institute of Standards and Technology (NIST) in coordination with federal entities, the private sector, academia, and other related actors, must establish guidelines for enhancing supply chain software security. These guidelines include a requirement for contractors to publicly provide a "Software Bill of Materials" – a formal record on the source of components used to build software – and disclose software vulnerabilities when discovered. The Order also asks the Director of NIST to define the term "critical software," outline security measures for critical software, and make available to agencies a list of categories of software that meet the definition of critical software. The Secretary of Homeland Security will take these guidelines to recommend amendments to the FAR to implement these guidelines. Software deemed critical that does not meet these guidelines will be removed from all indefinite delivery indefinite quantity contracts, Federal Supply Schedules, Federal Government-wide Acquisition Contracts, Blanket Purchase Agreements, and Multiple Award Contracts. This implementation is *retroactive* such that agencies using software developed or procured prior to the Order must comply with these requirements.

ESTABLISHING A CYBER SAFETY REVIEW BOARD

The Secretary of Homeland Security, along with the Attorney General, will establish a Board to review and assess significant cyber incidents and trigger establishment of a Cyber Unified Coordination Group during such incidents. The Board will include Federal officials from the Department of Defense, Department of Justice, CISA, the National Security Agency (NSA), the FBI, as well as private-sector cybersecurity and software suppliers. A representative of OMB will participate in Board activities should Homeland Security determine that a cyber incident involves Federal Civilian Executive Branch (FCEB) agency information systems.

STANDARDIZING THE FEDERAL GOVERNMENT'S RESPONSE TO CYBERSECURITY VULNERABILITIES AND INCIDENTS

The Director of CISA, in consultation with the Director of OMB, the Federal Chief Information Officers Council, the Federal Chief Information Security Council, Director of NSA, Attorney General, and Director of National Intelligence, will establish a standard set of operational procedures for responding to cybersecurity vulnerabilities involving FCEB Information Systems. These procedures will incorporate all appropriate NIST standards that all FCEB agencies will use and will be reviewed annually by the Director of CISA in consultation with the Director of NSA.

IMPROVING THE DETECTION OF CYBERSECURITY VULNERABILITIES AND INCIDENTS AS WELL AS INVESTIGATIVE AND REMEDIATION CAPABILITIES ON FEDERAL GOVERNMENT NETWORKS

FCEB agencies are to employ Endpoint Detection and Response (EDR) initiatives to support proactive detection of cybersecurity incidents. The Director of CISA will recommend options for these agencies to implement the EDR initiative and will require CISA to have access to agency data relevant to threat and vulnerability analysis. Further the Secretaries of Homeland Security and Defense are to share their agencies' response orders and emergency directives to ensure alignment between the Department of Defense Information Network and FCEB Information Systems directives. The agencies must also generate and preserve encrypted network and system logs to address cyber incidents and, upon request, provide these logs to the Director of CISA and FBI. Both Secretaries of Homeland Security and Commerce must formulate policies for logging retention and management.

CONCLUSION

The President's Order sets a broad agenda for federal agencies to improve cybersecurity and mitigate risk related to cyberattacks. Implementation of that agenda will take time, but the SolarWinds and Colonial Pipeline Company cyberattacks further emphasized the urgency for all federal agencies to move as quickly as possible and use the federal government's massive purchasing power to require its contractors and subcontractors to improve their networks,

products and services to better guard against cyberattacks. King & Spalding continues to closely monitor these developments and will update its client alerts as the Order is implemented.

The Executive Order may be accessed here.