President Biden Calls for Significant National Cybersecurity Improvements

President Biden recently signed an executive order, "Improving the Nation's Cybersecurity," signaling a significant increase in regulatory oversight of government contractors' cybersecurity programs. This action came on the heels of the Colonial Pipeline ransomware attack, which caused fuel shortages and panic across the East Coast of the United States, and just a few months after the massive Solar Winds breach. The executive order emphasizes the significance of protecting the country's information technology systems that underly the critical infrastructure for which U.S. citizens depend upon, and that "… the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security."

While the order only sets forth a few specific requirements concerning cybersecurity, it provides a detailed strategy for developing cybersecurity standards to be advanced by several agencies of the federal government including the Secretary of Defense, the Attorney General, the Secretary of Homeland Security and the Director of National Intelligence. Moreover, the order states that "all Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order." The order applies to both federal agencies and contractors and sets forth an aggressive timeline to meet the president's goals.

Highlights of the order include:

- **New IT Rules and Regulations for Federal Contractors:** Of utmost importance, the order calls for review and updates to the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation (DFAR) concerning Information Technology (IT) and cybersecurity. The recommendations must include descriptions of the contractors to be covered by the new language. Many changes in the order require additions or changes to the FAR.
- **Implementation of additional IT security measures:** Federal agencies are required to implement additional IT security measures, including movement to secure cloud servers, use of multifactor authentication and encryption, and centralizing and streamlining access to cybersecurity data to drive analytics and manage cybersecurity risks.
- **Enhance Software Supply Chain Security:** The order directs the establishment of baseline security requirements for software sold to the government. This includes requiring developers to make security data publicly available, resulting in greater transparency. Further, it calls for a public-private sector collaboration to develop new and advanced approaches to software development. Lastly, the order creates a labeling program so the government and public can determine whether software was developed securely.

- **Cyber Incident Reporting:** Certain government contractors will be required to report cyber incidents to federal agencies. The Director of Homeland security will recommend changes to the FAR, which will include the contractors and service providers covered, the nature of the cyber incidents that will require reporting, and the time periods for reporting based on "a graduated scale of severity." Specifically, the order states that for the most severe incidents, reporting will be required within three days.
- **Standardized government's incident response plan:** The order calls for the development of a standardized response plan and set of definitions for cyber incident response by federal departments and agencies. The order states that "standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses." The White House press release mentions the disparity within the government concerning cybersecurity response. This standardized response plan will require all agencies to meet a certain threshold and provide a template to the private sector for their response plans.
- **National Review Board:** Modeled after the National Transportation Safety Board, the Cybersecurity Safety Review Board will convene following a significant cyber incident to analyze the incident and make recommendations for cybersecurity improvements. The board will be co-chaired by both government and private sector leaders.

We will be monitoring these developments closely and provide updates as they become available. For more information concerning this information memo or other cybersecurity issues, contact Jessica Copeland, Shannon Knapp or any attorney in our Cybersecurity and Data Privacy practice.

BOND SCHOENECK & KING ATTORNEYS

Bond has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, www.bsk.com. Attorney Advertising. © 2021 Bond, Schoeneck & King PLLC.

Bond, Schoeneck & King, PLLC BondLawFirm Bond, Schoeneck & King bondlawfirm