protiviti®
Face the Future with Confidence

President Biden Executive Order to Strengthen U.S. Cybersecurity Will Impact Federal Agencies and Public and Private Sector Organizations

May 14,
2021

On May 12, President Joe Biden issued the Executive Order on Improving the Nation's Cybersecurity. This executive order (EO) is the most recent action by the administration to strengthen U.S. national cyber defenses and address cybersecurity threats and attacks that continue to grow in magnitude, impact and frequency. It is intended to protect networks in the federal, public and private sectors, and to strengthen the nation's ability to respond to cyber attacks when they occur, as well as to improve information sharing between the U.S. government and the private sector.

The EO is a step toward moving government action from response to attacks post-occurrence to prevention. It is the latest signal to all organizations doing business with the government that increased federal oversight and potential regulation of cybersecurity measures are coming.

The scope of the EO includes systems that process data, along with operational technology, whether cloud-based, on-premises or hybrid. Given that the United States is the world's largest buyer of IT services, the execution of the objectives detailed in this EO will impact federal agencies as well as a broad range of public and private sector organizations. The EO also calls for partnered efforts between the federal government and the private sector to foster a more secure cyberspace, calling on the private sector to adapt to the continuously changing threat environment and ensure its products are built and operate securely.

Increasing Cyberattacks Impact U.S. Companies and Infrastructure

The president's EO follows a series of malicious cyberattacks in the United States. In early 2020, a hack on SolarWinds' Orion remote IT management software infected the computer systems of more than 18,000 private and government customers. In February, a major water treatment system in Florida was breached, elevating sodium hydroxide levels to a point more suitable for household cleaners than human consumption. And most recently, a ransomware attack on the Colonial Pipeline on May 7 forced the company to temporarily

cease its operations and freeze IT systems, bringing the top U.S. fuel pipeline to a grinding halt and causing consumers to panic-buy gasoline, exposing the vulnerability of U.S. national and economic security. These and other cyber attacks – and the risk of future attacks that could damage the nation's critical infrastructure – compelled the president to implement a strict set of enhanced, more stringent standards on the cybersecurity capabilities of any software sold to the U.S. government.

Key Provisions of the Executive Order

The EO focuses on a number of important actions intended to bolster the nation's cybersecurity, several of which are summarized below. The full EO can be found here.

Removing barriers to sharing threat information between the public and private sector.

- The EO ensures that IT service providers are able to share information with the government and requires them to share certain breach information.

Protiviti's point of view: While much of the EO focuses on what the U.S. federal government will be doing, there are additional actions which will be required of private sector organizations to solve these issues. The EO focuses on the federal government, both as a consumer and a regulator – securing software, reporting and assisting in the response of cyber attacks, and participating in the Cybersecurity Safety Review Board (see below). As a regulator, the U.S. government will determine whether organizations meet these criteria. Public and private sector organizations can expect more rigid federal enforcement of these cybersecurity standards, and those organizations deemed to not be in compliance with these criteria may not be eligible to do business with the federal government.

Enhancing software supply chain security to improve the security and integrity of software used by the federal government.

- The EO will improve the security of software by establishing baseline security standards for development of software sold to the federal government, including requiring developers to maintain greater visibility into their software and making security data publicly available.

Protiviti's point of view: Over the course of the next 12 months, the Secretary of Commerce, in coordination with the Director of NIST, will develop and publish new criteria and guidelines for software security. Once these are developed, the federal government will

compel hardware and software companies to comply with them. In addition, the EO specifically addresses advancements in the automation of devices, which now spans a much broader range of industries and professions. New connected devices (e.g., IoT), enhanced speed (5G) and pushing automation to the production floor mean the necessary scope of security includes systems that process data, the operational technology running the vital machinery that ensures safety, and the devices that people wear on a daily basis. Organizations should anticipate and prepare for the potential for reporting requirements related to these baseline security standards by documenting current security procedures in preparation for potential review.

Establishing a Cybersecurity Safety Review Board to assist in and learn from high-profile attacks.

- The EO establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity.
- The board will review and assess threat activity, vulnerabilities, mitigation activities and agency responses.

Protiviti's point of view: Given the U.S. government's dependency on commercial software, a safety review board should assist with developing standards that provide thresholds for more secure software. Investigations conducted by this new safety review board will be analogous to investigations of accidents conducted by the National Transportation Safety Board. Organizations should anticipate additional guidance in the future on how to adhere to this provision.

Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents.

- The EO requires the development of a standardized set of operational procedures (i.e., playbook) to be used in planning and conducting cybersecurity and vulnerability response activity respecting FCEB information systems. The playbook will incorporate all appropriate NIST standards.
- The standardized procedures will ensure a more coordinated and centralized cataloging of incidents and tracking of agency processes to ensure more successful and appropriate responses.

- Agencies and private sector companies with procedures that deviate from the playbook must demonstrate that the procedures meet or exceed standards proposed in the playbook.

Protiviti's point of view: Organizations should use standardized (or approved) playbooks for responding to cybersecurity vulnerabilities and incidents. This is critical to having an effective response. Standard cybersecurity playbooks vary greatly depending on industry and size of company. Many organizations, particularly those that are not regulated, likely will need to enhance their current playbooks or move to develop them in line with these new standards.

Improving detection of cybersecurity vulnerabilities and incidents on federal government networks.

- The EO improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response system — something that does not exist today — and improved information sharing within the federal government.

Protiviti's point of view: The actions, recommendations and assignments in the EO should dramatically improve the intrusion detection capabilities on federal government networks. This is setting the direction and guidance to build the largest endpoint detection system in the world – far larger than anything that exists in the private sector.

Improving the federal government's investigative and remediation capabilities.

- The EO creates cybersecurity event log requirements for federal departments and agencies, which are intended to help investigators track the source of cyberattacks.

Protiviti's point of view: Given the increase in impacts, now is the time to improve forensics and investigative capabilities to ensure better preparedness and quicker remediations in the future. The nation's infrastructure needs to take these kinds of actions in order to be better prepared for future cyberattacks. It is clear the EO is going to push effective cyber hygiene as far as it can, mandating the move to multi-factor authentication (MFA), encryption at rest and encryption in transit. Additionally, organizations can anticipate increased use of the latest cybersecurity capabilities such as zero trust architecture, cloud computing and cloud security.

What's Next

Based upon an initial interpretation of the EO, organizations should anticipate new regulations, such as Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS), for those that do business with the U.S. federal government. Organizations can also expect new enforcement to ensure cybersecurity compliance, as well as new structures to enhance speed and coordination among federal agencies to respond to future incidents. This will have a trickle-down effect on all current security frameworks in federal agencies, as they will need to be revised to be in compliance with the EO's new cybersecurity standards. In turn, these standards will trickle down to organizations working with or receiving grants from the federal government.

How Protiviti Can Help

Protiviti can assist organizations with preparing to respond to the evolving threats posed by cyber attacks. Our professionals can:

- Help prepare, assess and remediate organizations' compliance with U.S. government data and privacy protection regulations including FAR, DFARS, NIST SP 800-53, NIST SP 800-171, and Cybersecurity Maturity Model Certification (CMMC).
- Assist organizations in properly evaluating, planning and executing the transition to a secure, modernized and efficient cloud computing environment.
- Assist with cybersecurity incident response planning, execution, emergency response and crisis management.
- Help organizations evaluate, plan and execute the transition to a zero trust architecture across their environment (e.g., in the cloud and on-premise) by implementing zero trust principles and adhering to guidance such as NIST 800-207.
- Assess, plan, implement and orchestrate MFA and encryption solutions to better protect digital assets.

To discuss further, reach out to Protiviti at IR@protiviti.com.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®