protiviti®
Face the Future with Confidence

New Executive Order Aims to Shore Up U.S. Cybersecurity Defenses

A Primer for Federal Government Contractors

On May 12, 2021, President Joe Biden signed an Executive Order (EO) to improve the United States' cybersecurity and protect federal networks. Following the SolarWinds breach and, most recently, the Colonial Pipeline ransomware attack, the EO is the most recent action in the Biden administration's plan to overhaul U.S. cybersecurity strategy and leadership, as signaled in a February 4, 2021, speech by Biden at the State Department, where he said, "We've elevated the status of cyber issues within our government, including appointing the first national – Deputy National Security Advisor for Cyber and Emerging Technology. We're launching an urgent initiative to improve our capability, readiness, and resilience in cyberspace."[1]

The EO is far from the first U.S. government mandate on cybersecurity – other executive orders and standards abound. The May 12 EO does introduce additional oversight and response capabilities by focusing on the following areas, with particular attention afforded to the role of information technology (IT) and operational technology (OT) service providers. Following is a brief summary of key sections in this latest EO:

- **Removing barriers to sharing threat information** – The federal government contracts with IT and OT service providers to conduct an array of day-to-day functions on federal information systems. The EO notes that removing contractual barriers and increasing the sharing of information about such threats, incidents and risks are necessary steps to accelerating incident deterrence, prevention and response efforts and to enabling

[1] www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/

more effective defense of agencies' systems and of information collected, processed and maintained by or for the federal government.

- **Modernizing federal government cybersecurity** – The federal government must take decisive steps to modernize its approach to cybersecurity, including by increasing its visibility into threats, while also protecting privacy and civil liberties. The federal government must adopt security best practices; advance toward zero trust architecture; accelerate movement to secure cloud services; centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in technology and personnel to match these modernization goals.
- **Enhancing software supply chain security** – The security of software used by the federal government is vital to its ability to perform critical functions. The federal government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.
- **Establishing a Cybersecurity Safety Review Board** – The federal government will establish 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.
- **Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incidents** – The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency (CISA) and in consultation with numerous federal government agencies and officials, will develop 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, which will incorporate all appropriate NIST standards, will ensure a more coordinated and centralized cataloging of incidents and tracking of agency processes, leading to more successful and appropriate responses.
- **Improving detection of cybersecurity vulnerabilities and incidents on federal government networks** – The federal government will employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing visibility into and detection of

cybersecurity vulnerabilities and threats to agency networks in order to bolster the federal government's cybersecurity efforts.

- **Improving the federal government's investigative and remediation capabilities** – Cybersecurity event log requirements will be imposed on federal departments and agencies. These requirements are intended to help investigators track the source of cyberattacks. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide them upon request to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.

The EO contains a number of specific obligations directed at federal government contractors and service providers. These include:

- Contract obligations to:
    - Collect and preserve data, information and reporting relevant to cybersecurity event prevention, detection, response and investigation on all information systems over which they have control, including systems operated on behalf of government agencies.
    - Share such data, information and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations and policies.
- Required collaboration with federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed.
- Required sharing of cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation.

Contractual arrangements will be effected through changes in the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) requirements and language for contracting with IT and OT service providers. These changes will

be proposed for public comment following a mandated review, within 60 days of the EO, by the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security and the Director of National Intelligence.

Information sharing protocols are required to be determined within 120 days of the EO by the Secretary of Homeland Security and the Director of the OMB.

The EO also subjects Information and Communications Technology (ICT) service providers to reporting requirements. Specifically, ICT service providers must promptly report cyber incidents involving a software product or service or a support system involving a software product or service to the agencies involved, and must also report directly to CISA, which is responsible for collecting and managing the information.

What These Changes Mean for Service Providers

Based upon the requirements of the EO, federal contractors and service providers should anticipate additional changes to FAR and DFARS. They also can expect new and enhanced 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, and in turn on all federal contractors, service providers, and state and local government organizations that receive federal funding.

While they await further direction, affected parties should, at a minimum:

- Ensure that they are properly protecting U.S. government data using the appropriate regulation found in their contracts (FAR, DFARS, FISMA, FedRAMP, NIST and CMMC).
- Follow the basic cybersecurity recommendations in the EO, such as multi-factor authentication (MFA), encryption and incident response plans.
- Confirm that their cloud providers, third party providers and sub-contractors are focused on the same controls.

About Protiviti's Services for Government Contractors and Government Organizations

Protiviti delivers new ways to tackle old and persistent challenges by combining a deep understanding of the issues facing organizations in the public sector with private sector best practices. We apply our years of experience working with organizations in both the private and public sectors to help government agencies solve today's problems.

With regard to cybersecurity, Protiviti's security solutions include reviews and assessments, incident response, security strategy, regulatory compliance, architecture, design, and implementation services. We help federal IT organizations address both known and emerging security and privacy risks through security reviews and related support. Our expert teams include Certified Information System Security Professional (CISSP) and Certified Information Privacy Professional for Government (CIPP/G) professionals. Their involvement ensures we deliver optimal control reviews that align with guidance from the National Institute of Standards and Technology (NIST), including FIPS-199, FIPS-201, NIST 800-60, NIST 800-53, NIST 800-171, NIST 800-40 series, Cybersecurity Maturity Model Certification (CMMC), Federal Information and Security Management Act (FISMA), and Federal Risk and Authorization Management Program (FedRAMP).