

Executive order on improving the nation's cybersecurity

Forensic & Integrity Services
Government Contract
Services

September 2021



In May 2021, President Biden issued an executive order on improving the nation's cybersecurity ("the Order"). The Order aims to modernize cybersecurity defenses by protecting federal networks, improving information sharing between the U.S. Government and private sector regarding cyber-related issues, and strengthening the ability to quickly respond to incidents when they occur.



Key highlights of the Order

The Order, is viewed as a response to the SolarWinds attack, contains several provisions that will impact organizations that contract with the U.S. Government. Some of the key highlights from the Order include:

Removing barriers to sharing threat information

The Director of the Office of Management and Budget (OMB) must review and recommend updates to the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement (DFARS) contracting language with information technology (IT) and operational technology (OT) service providers. The purpose of the review and subsequent recommendations is to ensure that IT and OT service providers entering into contracts with federal agencies promptly share certain cybersecurity breach information with the U.S. Government and increase public-private collaboration related to such incidents.

Modernizing federal government cybersecurity

The head of each agency shall update existing plans to prioritize resources for the adoption and use of cloud technology and develop a plan to implement zero-trust architecture. The Order also directs federal agencies to adopt certain security controls known to mitigate risks to sensitive data and systems, including multifactor authentication (MFA) and encryption for data at rest and in transit.

Enhancing software supply chain security

As directed by the Order, the Secretary of Commerce solicited input in June from the U.S. Government, private sector and academia to identify existing or develop new standards, tools and leading practices to enhance the security of the software supply chain. The Secretary of Commerce will subsequently issue guidance, incorporating feedback, identifying practices that enhance the security of the software supply chain, emphasizing the importance of security controls like segmentation, MFA, encryption, and endpoint detection and response tools (EDR).

Establishing a Cyber Safety Review Board

The Secretary of Homeland Security, in consultation with the Attorney General, shall establish the Cyber Safety Review Board, which will include both U.S. Government staff and private-sector representatives. The board is to be modeled after the National Transportation Safety Board and will be responsible for reviewing and assessing all cyber incidents with respect to agency information systems, excluding those for the Department of Defense (DoD) and intelligence community. The board is directed to provide recommendations to the President for improving cybersecurity and incident response practices upon completion of each incident review.

Standardizing the federal government's response to cybersecurity vulnerabilities and incidents

Within 120 days of the date of the Order, the Secretary of Homeland Security shall develop a standard set of operation procedures (referred to in the Order as the "federal government's playbook") to be used in planning and conducting cybersecurity vulnerability and incident response activities with respect to all agency systems, except those for the DoD and the intelligence community.

What does this mean for organizations contracting with the U.S. Government?

The Order will directly impact organizations that contract with the U.S. Government. Companies that provide IT and OT software or cloud services to the U.S. Government are likely to experience the most immediate impact of the Order, particularly as new requirements are incorporated into contracts. In addition to the impacts on organizations contracting with the U.S. Government and their supply chains, the downstream effects will likely impact the broader private sector as the cybersecurity standards set forth in the Order become industry leading practices. Certain initiatives, such as the increased adoption of zero-trust security and an accelerated movement to secure cloud services, will become more prominent components of network architecture, as organizations follow the model of the U.S. Government and its agencies.

For example, the Cyber Safety Review Board may play a significant role in drawing post-incident lessons learned that will guide public and private sector activities going forward. Additionally, the impact of the Order to be felt by manufacturers and operators of industrial systems, not just enterprise systems. U.S. Government contractors should expect additional guidance, as seen with the National Institute of Standards Technology white paper released on June 25, 2021, "[Definition of Critical Software Under Executive Order \(EO\) 14028.](#)"







The Order focuses on information-sharing requirements for DoD federal contractors or suppliers. However, non-DoD contractors will likely benefit from evaluating whether these changes will raise expectations for sharing cyber incident information with federal agencies. For example, businesses may benefit from tracking guidance and expectations regarding what information to share and when. Forthcoming guidance may help inform organizations contracting with civilian agencies with respect to how to manage information sharing, which can often be time-consuming while resources are stretched during the response to a cyber incident. Notably, while mentioning privacy considerations, the Order outlines expectations that increased sharing shall occur while adhering to privacy laws, regulations and policies.

Additionally, in section 2, subsection H of the Order it states, "Current cybersecurity requirements for unclassified system contractors are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the U.S Government." This could lay the groundwork for requiring the Cybersecurity Maturity Model Certification (CMMC) for contractors, regardless of the agency with which they contract.

Why Ernst & Young LLP?

Organizations that contract with the U.S. Government need to proactively and strategically manage their cybersecurity, as there will be a continued pressure to keep up with evolving standards and practices. As new requirements are released and existing ones such as CMMC evolve, contractors will need to adjust their approach to cybersecurity. With extensive cybersecurity resources constraints across commercial industries and the government and public sector, including professionals with intimate knowledge of government compliance structures, our professionals provide a holistic solution for CMMC compliance and readiness. Our experience in assisting defense contractors to comply with DFARS 252.204-7012 and CMMC has provided our clients with key insights into the challenges of implementing across diverse environments, as well as the additional considerations of data governance and subcontractor monitoring in the context of managing CUI. Our efforts enable organizations to manage risks, maintain compliance and maintain a proactive, rather than reactive, posture related to cybersecurity requirements.

Ernst & Young LLP Forensic & Integrity Services

	<p>Sajeev D. Malaveetil Practice Group Leader Government Contract Services +1 703 862 0543 sajeev.malaveetil@ey.com</p>		<p>Angel Contreras Principal Government & Public Sector +1 703 747 1428 angel.contreras@ey.com</p>
	<p>Mustafa Zuwawa Senior Manager Government Contract Services +1 949 437 0703 mustafa.zuwawa@ey.com</p>		<p>Danielle Dalton Senior Manager Business Consulting +1 206 262 6418 danielle.dalton@ey.com</p>
	<p>Timothy Manning Senior Manager Government Contract Services +1 617 375 8355 tim.manning@ey.com</p>		<p>Michael Hinckley Senior Manager Business Consulting +1 615 252 2124 michael.hinckley@ey.com</p>

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity.

Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2021 Ernst & Young LLP.
All Rights Reserved.

SCORE no: 13553-211US
2107-3824155
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/forensics/governmentcontractservices