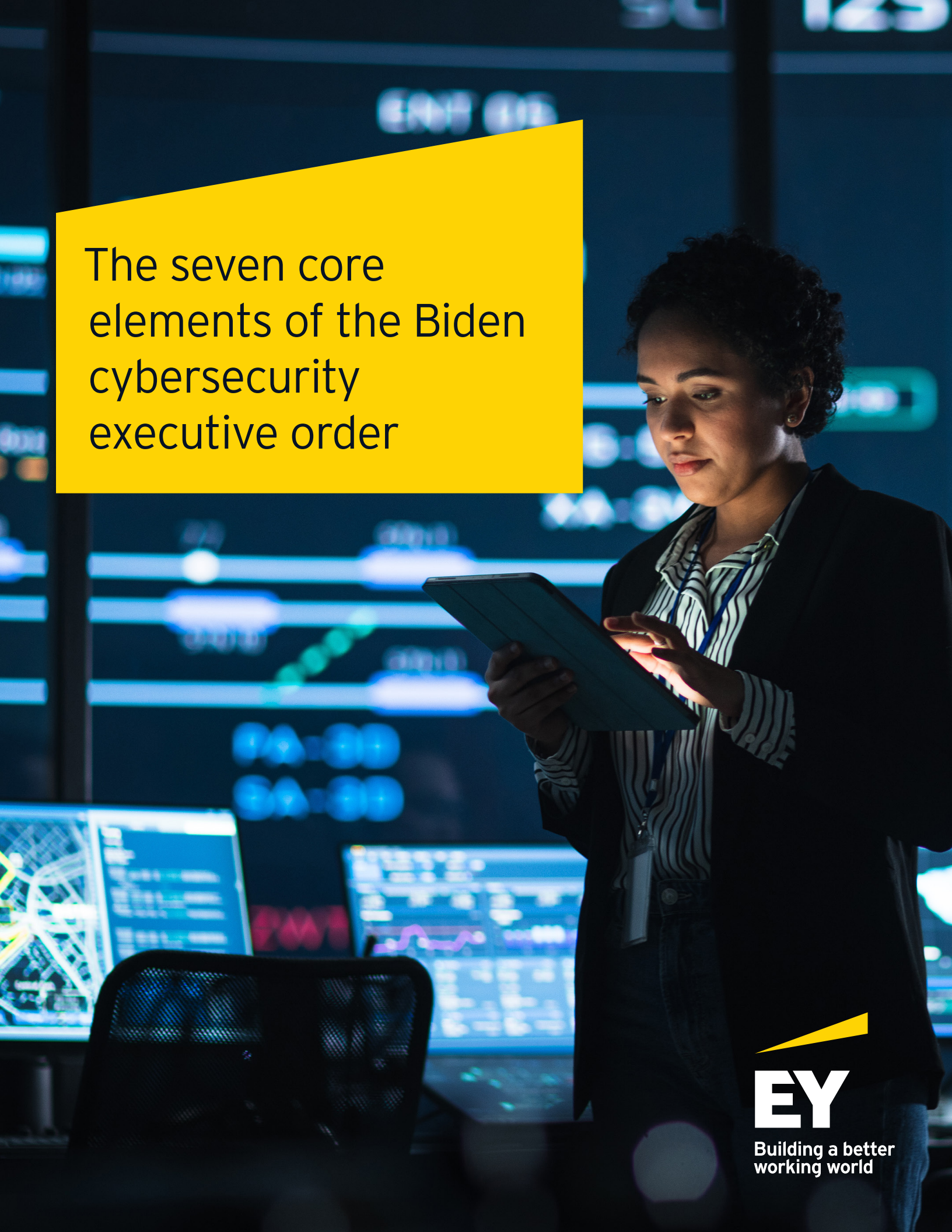
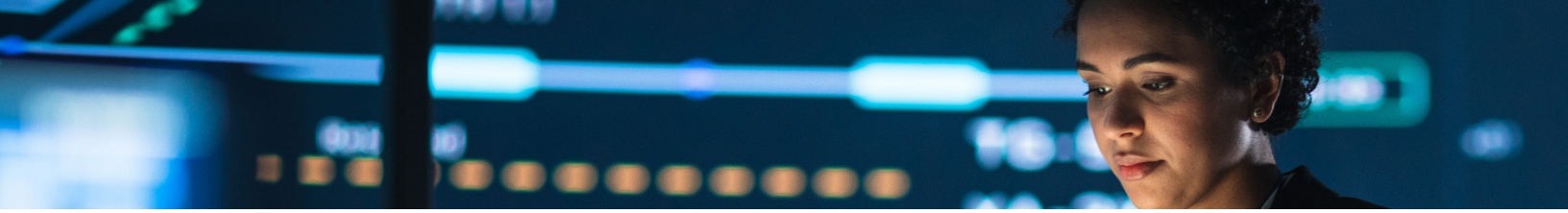
The seven core elements of the Biden cybersecurity executive order



Building a better working world



On 12 May 2021, President Biden signed an Executive Order aimed at protecting federal government networks and modernizing the nation's overall cybersecurity. The seven core elements of the Executive Order are:

Seven core elements

1. **Enhancing threat information sharing**

   Requires federal contracts be updated and standardized to require service providers to collect and share cyber threat and incident information with the agency they have contracted with, as well as others like the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI).

2. **Modernizing the federal government's cybersecurity**

   Requires Federal agencies to adopt security practices such as multi-factor authentication, encryption of data in motion and at rest, and Zero Trust architecture. Encourages faster adoption of secure cloud services and streamlining access to cybersecurity data to drive analytics for identifying and managing cyber risks.

3. **Enhancing software supply-chain security**

   Directs the National Institute of Standards and Technology (NIST) to develop guidelines and criteria to evaluate software security, including the security practices of developers and suppliers, and methods to demonstrate conformity with secure practices. Requires development of a definition of "critical software" and would require federal agencies to verify that future software procurements meet security guidelines. This section also directs the establishment of consumer product labeling programs to help educate the public about the security capabilities of Internet of Things (IoT) devices.

4. **Cyber Safety Review Board**

   Establishes a public-private review board to assess significant cyber incidents (as defined by PPD-41). The Board's first review will be of SolarWinds activity and to provide recommendations for improving cybersecurity and incident response capabilities.

5. **Standardizing federal playbooks**

   To provide for a more coordinated and centralized catalog of incidents and tracking of federal agencies' remediation efforts, requires development of a standard set of operating procedures to be used across the federal government for planning and conducting a cyber incident response activity.

6. **Improving detection on federal networks**

   Focuses on maximizing early detection of cyber threats and vulnerabilities on federal networks and systems by requiring all federal civilian agencies (defense and intelligence would be handled separately) to deploy an Endpoint Detection and Response initiative to promote detection, active threat hunting, containment, remediation and incident response.

7. **Improving investigative and remediation capabilities**

   Requires the development of recommendations to improve the logging of events and incident data retention on federal systems and those hosted by third parties such as cloud services providers. Requires such data be shared with CISA and the FBI upon request.

How EY teams can help

Whether your organization is directly affected by the cybersecurity executive order, or you want to take advantage of this new set of data in your third-party risk management (TPRM) program, EY Consulting can help you take action to improve your cybersecurity posture with customized approaches for your organization, including:

- Software supply-chain security
- Cyber threat intelligence
- Third-party risk management
- Business resiliency
- Cyber risk management and planning
- Privileged access management
- Identity and access management
- Detecting and responding to active threats
- Incident response planning exercises

Contact us for more information on the Biden cybersecurity order and protecting your organization from cybersecurity threats.

Kris Lovejoy
EY Global Cybersecurity Leader
kristin.lovejoy@eyg.ey.com

Dave Burg
EY Americas Cybersecurity Leader
dave.burg@ey.com

Mike Maddison
EY EMEIA Cybersecurity Leader
mike.maddison@uk.ey.com

Richard Watson
EY Asia-Pacific Cybersecurity Leader
richard.watson@au.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to 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.

EYG no. 005651-21Gbl
2106-3788310
ED None

ey.com