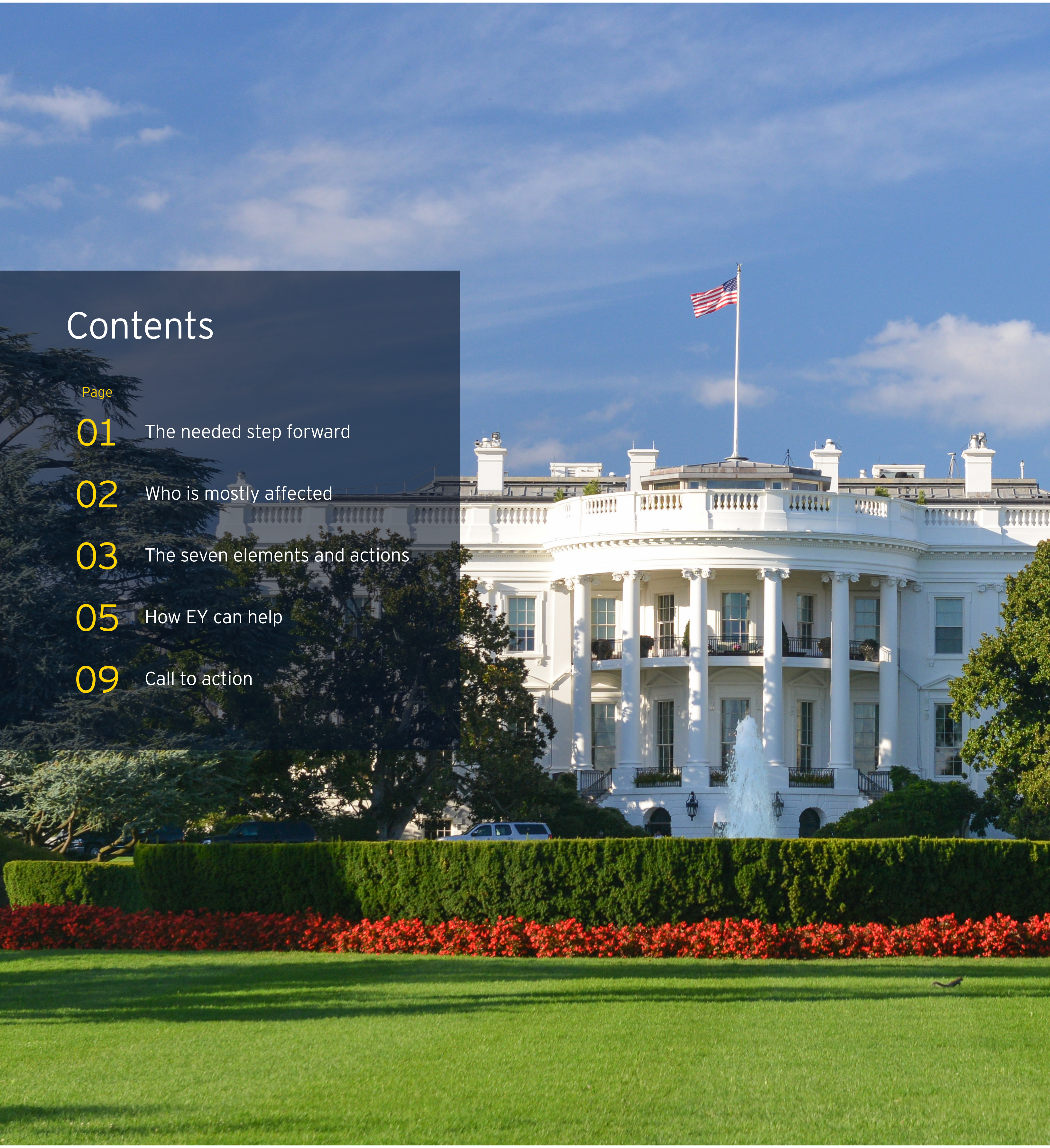
President Biden's Executive Order: the next step toward cybersecurity modernization

October 2021

EY
Building a better
working world



Contents

The needed step forward

Federal agencies must understand the actions needed and the added level of responsibilities the EO enacts regarding threat information sharing, modernizing cybersecurity and building a secure cyberspace.

President Biden's Executive Order (EO) on cybersecurity is designed to deliver a needed modernization of the continually evolving cybersecurity defenses and improved protection of federal government networks. The EO comes amid increasingly public and widespread cyber attacks that have created malicious data breaches and implemented ransomware as their attack vector and fully illustrates the vulnerability, exposure, ramifications and need to take immediate action. The Biden administration recognizes the inherent risks, and the EO is designed to improve the government's efforts to identify, deter, protect against, detect and respond to the actors and their actions. All organizations — and specific to this article, federal agencies — should consider their approach to the EO and plan a strategic path forward.

Federal agencies must understand the actions needed and the added level of responsibilities the EO enacts regarding Federal Acquisition Regulation (FAR) and Department of Defense FAR Supplement (DFARS). The EO drives new guidelines and processes that are expected within the year and will likely become new industry standards with global outcomes and reach. Federal contractors must consider how they will be affected by the EO, examining their software supply chain security and third-party risk management.

Who is mostly affected

While the aim of the EO is far-reaching, its inception generally affects three segments.

1. Federal agencies are expected to immediately modernize their technology environment and security practices.
2. Federal contractors will see new cybersecurity standards built into contract terms, including commercial-off-the-shelf (COTS) software providers. The primary focus is to require all stakeholders to share more information in a faster manner concerning all cyber incidents.
3. The private sector will see an immediate shift and focus on software supply chain security. This will include increased transparency through consumer security labeling on software and IoT devices. This shift means developers of software and IoT device companies will experience new security requirements and assessment standards.

The EY Cybersecurity practice is keenly positioned to help federal agencies understand, plan for and implement cyber that address the objectives of the EO. Our teams have the proven proficiency and experience to help federal agencies more accurately quantify their cyber risk, capture detail about prioritizing investments and capabilities, and chart the processes and steps needed to insert leading-edge security, privacy and resilience into digitally enabled initiative and government networks moving forward. As the preliminary guidelines from the National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), and Office of Management and Budget (OMB) take shape and the details are offered, the EY Cybersecurity practice can help federal agencies prepare for and strategically implement the actionable measures needed to implemenet changes and fully leverage significant investments in order to defend the vital institutions that underpin the American way of life.

The seven elements and actions

Seven core elements

1. Enhancing threat information sharing
2. Modernizing the federal government's cybersecurity
3. Enhancing software supply chain security
4. Cyber Safety Review Board
5. Standardizing federal playbooks
6. Improving detection on federal networks
7. Improving investigative and remediation capabilities

The EO's objectives, structured around modernization, information sharing and gaining control, have seven core elements, which include a number of agency-specific actions to strengthen federal government networks.

1. Enhancing threat information sharing

Specifies that 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).

Agency-specific actions

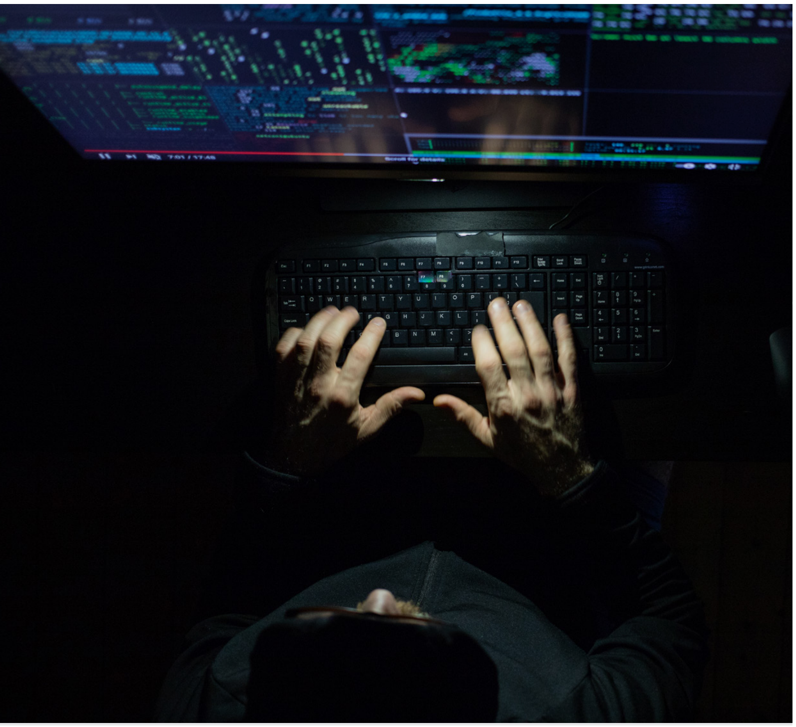
- Update and standardize federal contracts per revised FAR/DFAR contract requirements.

2. Modernizing the federal government's cybersecurity

Requires federal agencies to adopt security practices such as multifactor authentication (MFA), 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.

Agency-specific actions

- Update existing agency plans to prioritize resources for the adoption and use of cloud technology.
- Develop a plan to implement zero trust architecture.
- Implement MFA and encryption for data in rest and transit.



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 obligate 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.

Agency-specific actions

- Remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts and issuing guidance identifying practices that enhance the security of the software supply chain.

4. Cyber Safety Review Board

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

Agency-specific actions

- Participate in Cyber Safety Review Board (CSRB) as needed basis.

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.

Agency-specific actions

- Issue guidance on use of the federal playbook for planning and conducting a cybersecurity vulnerability and 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 (EDR) initiative to promote detection, active threat hunting, containment, remediation and incident response.

Agency-specific actions

- Deploy an EDR initiative and establish or update memoranda of agreement (MOA) with CISA for the Continuous Diagnostics and Mitigation Program to make object, level data, as defined in the MOA, available and accessible to CISA.

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. Also requires such data be shared with CISA and the FBI upon request.

Agency-specific actions

- Institute and comply with Department of Homeland Security (DHS) policies to establish requirements for logging, log retention and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency.

While there is an independence of each core element, there is a unifying overlapping theme that forges the efforts toward a shared outcome: modernization and improved protection for government networks.

How EY can help

The EY Cybersecurity practice recognizes that the EO is the first step to gaining control and modernizing cybersecurity defenses and protecting federal government networks. The EO is not a set rule, but a model to build upon and guide federal agencies forward to the next phase to bolster the nation's security in multiple infrastructure sectors. The EY Cybersecurity practice has four strategic cyber capabilities to help federal agencies plan, track and manage accordingly to meet the EO requirements and position cyber teams for ongoing change.

Cyber capabilities to meet EO requirements

1. Zero Trust

Zero trust architecture is a security paradigm that fixes the inherent weakness of conventional strategies that only data outside an entity needs to be secured. This new paradigm requires the organization to continuously analyze and evaluate the risks involving its internal IT assets and business functions and to form strategies to mitigate them. The zero-trust approach is most effective when it's extended throughout the digital landscape and used as an integrated security strategy. This is done by implementing zero trust controls and technologies across six foundational elements: people, devices, applications and services, infrastructure, networks, and data.

Please **click here** for EY's POV on Zero Trust adoption.

For a deeper dive on identity centric Zero Trust Architecture implementation, **click here**.

Zero trust building blocks and capabilities

The zero trust approach is most effective when it's extended throughout the entire digital landscape and used as an integrated security strategy. This is done by implementing zero trust controls and technologies across six foundational elements:

1 People

2 Devices

3 Applications and services

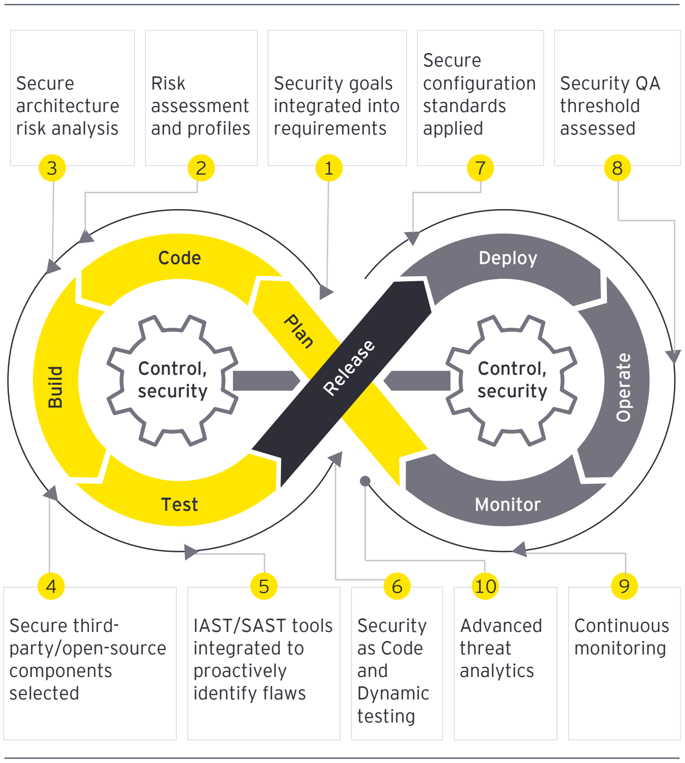
4 Infrastructure

5 Networks

6 Data

2. Secure Software Development

Security and integrity of critical software are going to become high priorities. Suppliers must provide a software bill of materials, similar to FDA requirements for medical devices. Other than software bill of materials (SBOM) requirements and critical software identification, public, private and government sector will collaborate in vulnerability disclosure programs going forward. Secure software development life cycle (SSDLC) and continuous integration/continuous delivery (CICD) pipeline guidelines are going to be revised by NIST, and new standards are going to be published. Agencies should apply a risk-based approach when implementing security controls in the software development pipeline. Additionally, automation via security as code can enable detection and verification of security risks. Organizations moving critical software to the cloud should take the opportunity to implement baseline security controls and apply verification checks as part of the pipeline.


Secure architecture risk analysis
3
Risk assessment and profiles
2
Security goals integrated into requirements
1
Secure configuration standards applied
7
Security QA threshold assessed
8
Code
Plan
Build
Control, security
Test
Release
Deploy
Control, security
Operate
Monitor
4
Secure third-party/open-source components selected
5
IAST/SAST tools integrated to proactively identify flaws
6
Security as Code and Dynamic testing
10
Advanced threat analytics
9
Continuous monitoring

3. End point detection and response

Although highly effective at threat prevention, detection and mitigation, an endpoint detection and response tool is just one component of your larger defense-in-depth strategy. The current ecosystem of EDR tools offers vastly different capabilities, each with its own benefits and drawbacks that must be considered in the context of your overall defensive posture. Key capability areas include:

- Data: What data is captured, where is it processed, and how long is it retained?
- Automation: Does the tool support automated actions like process/connection blocking, host isolation and artifact collection?
- Intelligence: Does the tool support vendor-provided or third-party intelligence integration, such as signatures, hunting queries and indicators of compromise?

The EY's approach to implementing an EDR solution consists of four phases:

1. Identification: Narrowing the focus to tools whose capabilities best complement your defensive posture
2. Selection: Evaluating the identified tools based on unique environmental factors, network architecture, and capabilities/gaps
3. Planning: Accounting for physical, logical, and business factors to create a deployment plan that prioritizes risk minimization
4. Deployment: Installing agents and updating environment configurations to enable EDR capabilities

The rapidly evolving threat landscape means a default, out-of-the-box solution will not be sufficient; further, even a tailored solution will, over time, become stale and inadequate. Thus, the following should also be performed immediately after deployment and periodically thereafter:

5. Assessment & Customization: Assessing the efficacy of your overall defensive posture, including the EDR, to support threat prevention, detection, mitigation, and response. The EY's methodology combines intelligence-driven threat scenarios with a robust breach and attack Simulation (BAS) tool (e.g., AttackIQ or Mandiant Security Validation).

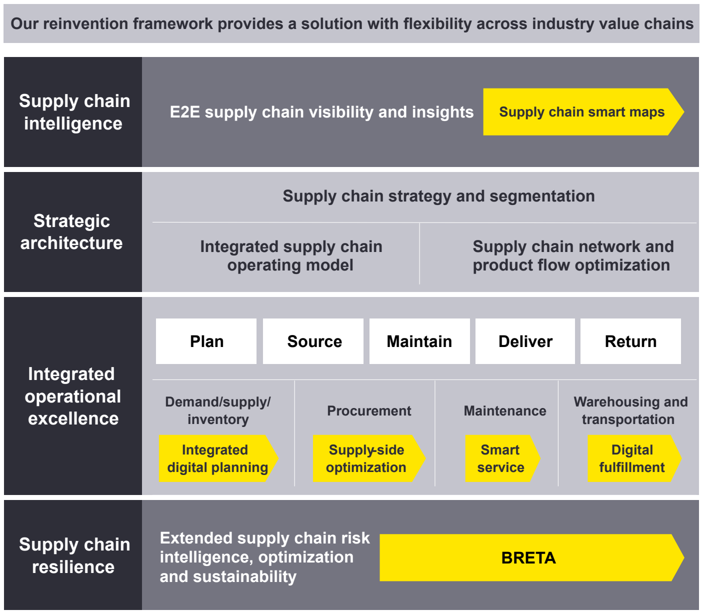
Alliances with leading EDR vendors, including **CrowdStrike** and **Tanium**, inform the EY approach.

4. Supply chain risk management

Government agencies are faced with big challenges as they continue to leverage suppliers for products and services to meet their missions. Failing to address the vulnerabilities of supply chains could expose agencies to risk that could impact their mission. Establishing a supply chain risk management (SCRM) program that enables leadership to make risk-informed decisions and reduce the risk introduced by suppliers is a key step towards managing risks of suppliers. The SCRM program identifies, assesses, helps to mitigate and monitors supplier risks: the greater the potential risk a supplier presents to agency's supply chain, the greater the diligence conducted to assess the supplier. The program assesses suppliers across multiple risk lenses to include financial, cybersecurity, geopolitical, corruption and foreign interest. Applying multiple lenses enables a more complete picture of the health of the supplier.

Please **click here** for EY's POV on resillient supply chain.

Key steps to building supply chain resilience



Our reinvention framework provides a solution with flexibility across industry value chains

Supply chain intelligence
E2E supply chain visibility and insights
Supply chain smart maps

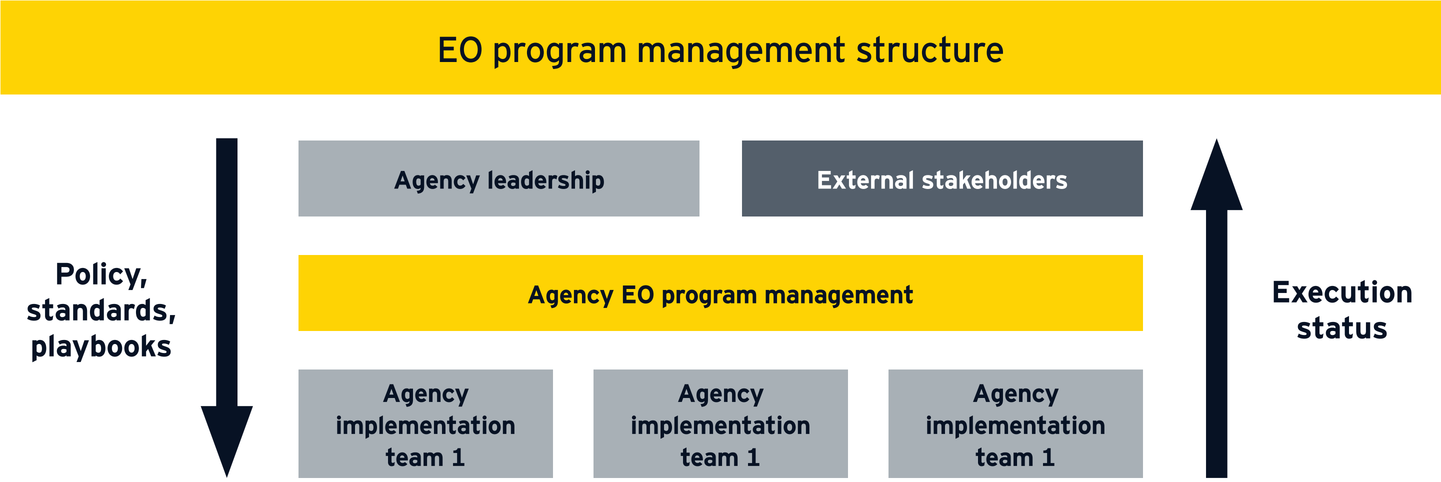
Strategic architecture
Supply chain strategy and segmentation
Integrated supply chain operating model
Supply chain network and product flow optimization

Integrated operational excellence
Plan
Source
Maintain
Deliver
Return
Demand/supply/ inventory
Integrated digital planning
Procurement
Supply-side optimization
Maintenance
Smart service
Warehousing and transportation
Digital fulfillment

Supply chain resilience
Extended supply chain risk intelligence, optimization and sustainability
BRETA

EO planning and track

Because the implicit challenges that extend from the reach and scope of the EO – and the importance of meeting these requirements – are complex and complicated, agencies would benefit from creating and having in place a dedicated project management team that can track status; manage cost, scope and schedule challenges; and communicate with internal and external stakeholders. This approach to planning, managing and tracking actions against the EO policies, standards and playbooks involves discussions with federal agency leaders, external stakeholders and agency EO program management teams. By tracking the status and actions taken, and viewing stages and progess made via an agency EO dashboard, agencies can input and visualize real-time requests, changes and status.



EO program management structure

Policy, standards, playbooks

Agency leadership

External stakeholders

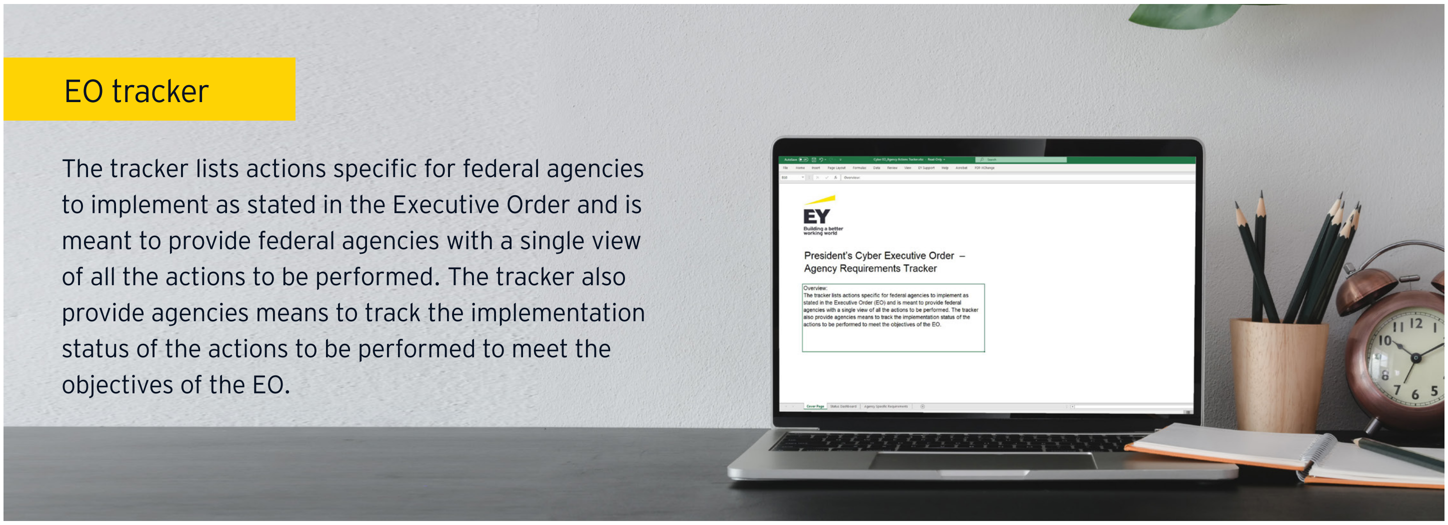
Agency EO program management

Agency implementation team 1

Agency implementation team 1

Agency implementation team 1

Execution status



EO tracker

The tracker lists actions specific for federal agencies to implement as stated in the Executive Order and is meant to provide federal agencies with a single view of all the actions to be performed. The tracker also provide agencies means to track the implementation status of the actions to be performed to meet the objectives of the EO.

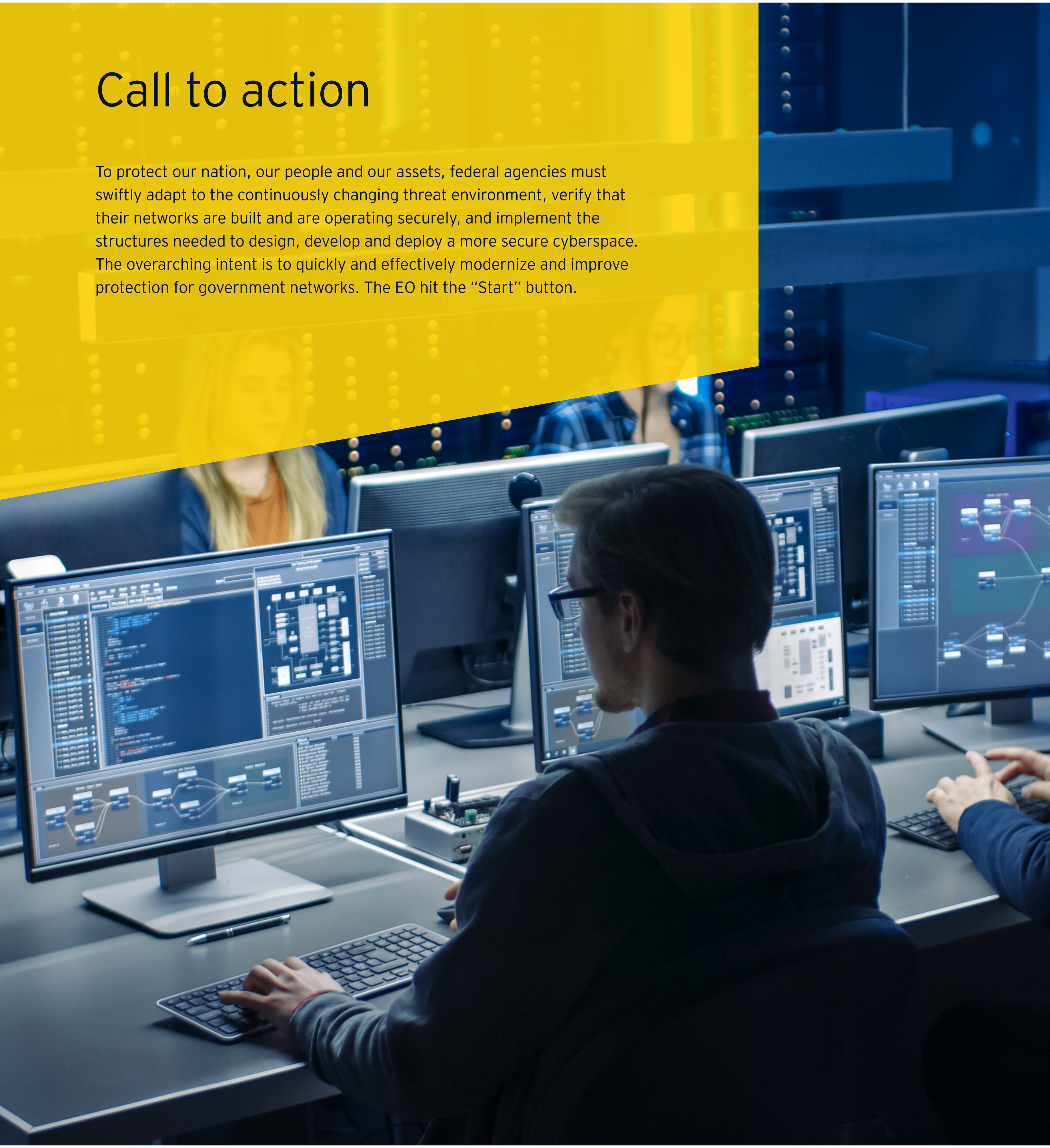
Cyber EO_Agency Actions Tracker.xlsx - Read-Only
File
Home
Insert
Page Layout
Formulas
Data
Review
View
EY Support
Help
Acrobat
PDF-XChange
EY
Building a better working world
Cover Page
Status Dashboard
Agency Specific Requirements

President's Cyber Executive Order – Agency Requirements Tracker

Overview:
The tracker lists actions specific for federal agencies to implement as stated in the Executive Order (EO) and is meant to provide federal agencies with a single view of all the actions to be performed. The tracker also provide agencies means to track the implementation status of the actions to be performed to meet the objectives of the EO.

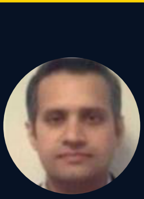
Call to action

To protect our nation, our people and our assets, federal agencies must swiftly adapt to the continuously changing threat environment, verify that their networks are built and are operating securely, and implement the structures needed to design, develop and deploy a more secure cyberspace. The overarching intent is to quickly and effectively modernize and improve protection for government networks. The EO hit the "Start" button.



EY contacts

Scott Smith
EY Government and Public Sector
Cybersecurity Leader
scott.smith5@ey.com



Anuj Tripathi
EY Government and Public Sector
Technology Consulting
anuj.tripathi@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.

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.

SCORE no. 14376-211US
2108-3843739
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