A NEW CYBER STANDARD

Preparing for the White House's Executive Order on Cybersecurity

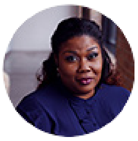
In May 2021, the White House signed an executive order (EO) aimed at improving the nation's cybersecurity across the public and private sectors. As changes come into effect over the coming months, federal and commercial organizations will need to quickly navigate new security requirements surrounding zero-trust architecture, multi-factor authentication, **threat information sharing**, and supply chain risk management.

Our own Dr. Shayla Treadwell, executive director of governance, risk, and compliance, and Keith McCloskey, chief technology officer of ECS' homeland security sector, sat down to discuss the law's impacts and how ECS can help organizations achieve compliance with the new EO.

SHAYLA TREADWELL
Executive Director, Governance, Risk, and Compliance

KEITH MCCLOSKEY
Chief Technology Officer, Homeland Security Sector

Q: WHAT IS THE IMPORTANCE OF THE CYBERSECURITY EO?



Shayla Treadwell: To combat the growing threat of cyberattacks, the government is seeking to modernize the cybersecurity of federal organizations and the companies that supply them. The recent high-profile attacks on SolarWinds and the Colonial Pipeline have laid bare the urgent need to protect the nation's critical infrastructure. By strengthening the entire supply chain and enhancing the government's threat intelligence and detection and response capabilities, this EO seeks to "defend the vital institutions that underpin the American way of life" by leveraging the combined power of the nation's federal and commercial enterprises.

Q: HOW WILL THE EO IMPACT DIFFERENT INDUSTRIES?

Keith McCloskey: The White House's EO will have far-reaching effects on both the public and private sectors. In the federal government, each agency head will now be responsible for assessing departmental risk and implementing protective security measures such as **zero-trust architecture** and multi-factor identification. The EO also calls for an accelerated shift to **secure cloud**.

For federal contractors, including commercial-off-the-shelf (COTS) software providers, new cybersecurity standards will be built into contract language. Contractors will now be required to collect, preserve, and share information related to cyber threats and promptly report the discovery of cyber incidents. By removing the contractual barriers around information sharing, the government hopes to improve interagency **threat intelligence and response**.

EXECUTIVE ORDER KEY GOALS

Remove Barriers to Threat Information Sharing Between Government and the Private Sector

Modernize and Implement Stronger Cybersecurity Security Standards in the Federal Government

Improve Software Supply Chain Security

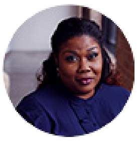
Establish a Cyber Safety Review Board

Create a Standard Playbook for Responding to Cyber Incidents

Improve Investigation and Remediation Capabilities

New baseline security standards will also govern how private industry develops and sells software to the government. All software will need to meet higher production standards aimed at **increasing supply chain security** and strengthening products' ability to resist cyberattacks. The EO also creates a new consumer labeling program to incentivize the market into protecting the security and privacy of customers and individuals. Technology companies will need to **adapt their development practices** to meet these new security standards.

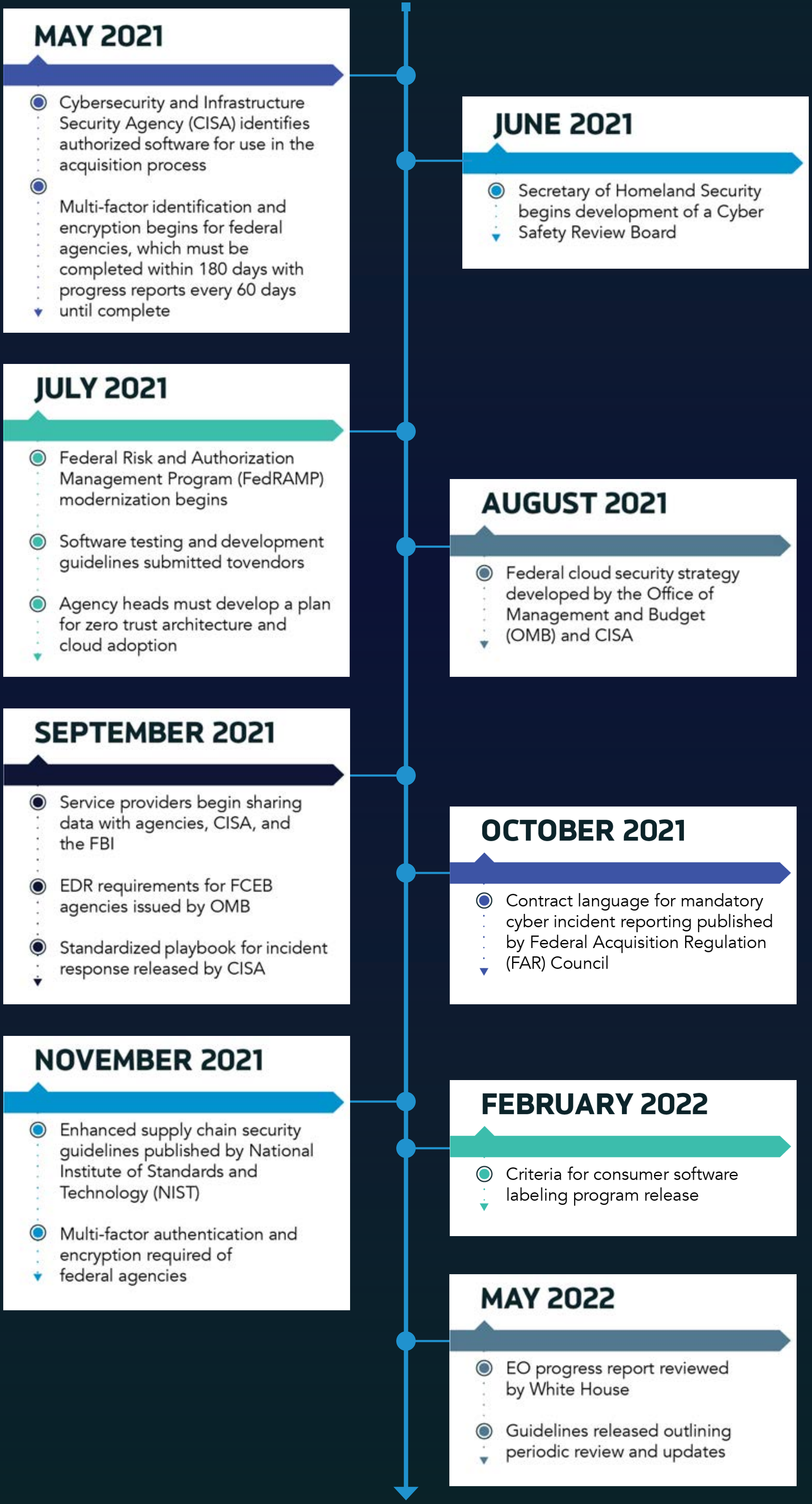
Q: WHEN SHOULD ORGANIZATIONS EXPECT THESE CHANGES?



Shayla: The EO's accelerated timeline reflects the importance and necessity of these new cybersecurity measures. Federal organizations will need to quickly assess the state of their cyber postures and **modernize many of their legacy systems** within the first six months of the EO signing. Guidelines for commercial enterprises will quickly follow, taking effect within the year. The EO's rapid timeline and technical challenges mean federal and commercial enterprises will need to rely heavily on their contractors and partners to enact the required security solutions.

The biggest challenge facing federal organizations will be the adoption of **zero-trust architecture**, multi-factor authentication, and the new requirements surrounding information sharing standards. The Defense Industrial Base (DIB) will face slightly different challenges given their added supply chain requirements. Suppliers will need to implement automation and development security operations (**DevSecOps**), both necessary components of data collection, logging, and secure software development.

WHITE HOUSE'S EXECUTIVE ORDER TIMELINE



MAY 2021

- Cybersecurity and Infrastructure Security Agency (CISA) identifies authorized software for use in the acquisition process
- Multi-factor identification and encryption begins for federal agencies, which must be completed within 180 days with progress reports every 60 days until complete

JUNE 2021

- Secretary of Homeland Security begins development of a Cyber Safety Review Board

JULY 2021

- Federal Risk and Authorization Management Program (FedRAMP) modernization begins
- Software testing and development guidelines submitted tovendors
- Agency heads must develop a plan for zero trust architecture and cloud adoption

AUGUST 2021

- Federal cloud security strategy developed by the Office of Management and Budget (OMB) and CISA

SEPTEMBER 2021

- Service providers begin sharing data with agencies, CISA, and the FBI
- EDR requirements for FCEB agencies issued by OMB
- Standardized playbook for incident response released by CISA

OCTOBER 2021

- Contract language for mandatory cyber incident reporting published by Federal Acquisition Regulation (FAR) Council

NOVEMBER 2021

- Enhanced supply chain security guidelines published by National Institute of Standards and Technology (NIST)
- Multi-factor authentication and encryption required of federal agencies

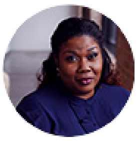
FEBRUARY 2022

- Criteria for consumer software labeling program release

MAY 2022

- EO progress report reviewed by White House
- Guidelines released outlining periodic review and updates

Q: HOW DO ORGANIZATIONS MEET THE CHALLENGES OF THE NEW EO?



Shayla: In order to implement the order's new cybersecurity requirements, the government and its partners will need to work alongside contractors to modernize cybersecurity services across the entire federal ecosystem. Achieving compliance is a process that requires understanding an organization's systems, processes, and protocols before developing roadmaps and strategies to strengthen their cybersecurity posture.

ECS

BUYER'S GUIDE

Cybersecurity Maturity Model Certification Preparation

Similar to our **Cybersecurity Maturity Model Certification** (CMMC) compliance services, ECS builds custom-tailored solutions to meet your organization's specific needs. Our technical subject matter experts (SMEs) work hand in hand with chief information security officers (CISOs), executives, and other IT leaders to implement the missing technologies, capabilities, and practices required by the new EO.

Keith: ECS is already helping customers respond to key aspects of the cybersecurity EO. Right now, our experts are working with federal security agencies to develop new logging requirements and implement continuous diagnostics and mitigation (CDM) dashboards for the effective use of EDR data.

As a recognized industry leader in cybersecurity, cloud, and artificial intelligence (AI), ECS has the managed security solutions to help our customers adhere to all the requirements of the new EO. From federal agencies to state governments, Fortune 500 companies, and small cap businesses, we work with customers to automate nearly every aspect of cyber analytics, vulnerability management, threat hunting, and incident response. Our advanced cyber threat defense solutions have the capability to protect up to 1.4 million Department of Defense (DoD) endpoints, and with our 24/7/365 managed security operations center (SOC), ECS already practices the intelligence sharing required by the EO. Our security and software engineers are experts in **DevSecOps** development, crafting secure pipelines for open-source software, machine learning algorithms, training environments, and more.

With over 30 years' experience delivering information technology (IT) solutions to federal and commercial customers, ECS is well-positioned to help protect our nation's most critical infrastructure. Whether the challenge is **modernizing legacy systems** for the cloud, implementing zero-trust architecture, or enacting **threat information sharing and intelligence**, ECS has the expertise to help your enterprise defend its networks, develop secure applications, and meet the new federal guidelines.

Interested in learning about our cybersecurity, cloud, and compliance solutions?
Reach out and **talk to an expert** today.

AUTHOR PROFILE

Shayla Treadwell
Executive Director, Governance, Risk, and Compliance

CONTACT OUR EXPERTS