CyberRes

Fulfilling the Executive Order on Cybersecurity

Cyber Resilience for Federal Agencies

An Executive Order... Now What?

You need an advantage. Better yet, a partner.

President Biden's Executive Order on Improving the Nation's Cybersecurity is welcome in light of the many security breeches and ransomware attacks we have all recently seen in the news. Now, your federal agency has mandates to meet, with specific due dates and technology requirements. What are you going to do?

CyberRes is one of the only companies that fully meets all eight technology mandates of the 47 sections of the Executive Order. With more than 40 years of experience across 40,000 customers, we have the technology and the services you need to meet your deadlines today, and strengthen your cyber resilience for tomorrow.

We're not just a vendor. We're your partner to help you protect, detect, and evolve your cyber resilience.

Section 3

Modernizing Federal Government Cybersecurity

Executive Order Language

Each agency shall develop a plan to implement a NIST-oriented Zero Trust Architecture and present to OMB and APNSA.

Products

NetIQ

Timing

July 20, 2021

Executive Order Language

Evaluate the types and sensitivity of agency's unclassified data, with prioritization of the unclassified data considered by the agency to be the most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data.

Products

Voltage, Secure Content Management, Universal Discovery

Timing

July 20, 2021

Executive Order Language

Agencies shall adopt multi-factor authentication and encryption for data at rest and in transit…

Products

NetIQ, Voltage

Timing

November 17, 2021

NetIQ

An integrated platform for adaptive identity, access, and privilege management to drive modern IT ecosystems.

Voltage

Protect sensitive structured and unstructured data to reduce breach risk with privacy-enabled data usability across hybrid IT.

Secure Content Management

Know what data you've stored, who has access to it, and what policies are most effective in managing it.

Universal Discovery

UD delivers end-to-end IT visibility through an agent, agentless, and/or passive deployment in any cloud, on-premise, or hybrid IT environment.

Section 4

Enhancing Software Supply Chain Security

Executive Order Language

Issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding secure software development environments, including such actions as: using administratively separate build environments; auditing trust relationships; establishing multi-factor, risk-based authentication and conditional access across the enterprise; documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software; employing encryption for data; monitoring operations and alerts and responding to attempted and actual cyber incidents; generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes; employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code; employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release; providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated; maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis; providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website; participating in a vulnerability disclosure program that includes a reporting and disclosure process; attesting to conformity with secure software development practices; ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

Products

Fortify, Sonatype

Timing

August 19, 2021

Fortify

Automate testing throughout the CI/CD pipeline so developers can quickly resolve issues and build secure software fast.

Sonatype

Sonatype delivers 10x faster feedback loops ensuring code quality, and that open source libraries are secure and compliant

Section 7

Improving Detection of Cybersecurity Vulnerabilities on Federal Government Networks

Executive Order Language

Issue requirements for FCEB Agencies to adopt Federal Government-wide EDR approaches, to support a capability of engage in cyber hunt, detection, and response activities.

Products

ArcSight

Timing

June 20, 2021

Executive Order Language

Deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

Products

ArcSight

Timing

August 19, 2021

ArcSight

Get faster, more accurate detection of known and unknown threats with a security analytics-powered SOC that intelligently adapts to talent shortages.

Section 8

Improving the Federal Government's Investigative and Remediation Capabilities

Executive Order Language

Provide requirements for logging events and retaining data within an agency's systems and networks, including the types of logs, retention period, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. Logs shall be protected by cryptographic methods to ensure integrity once collected and periodically verified against the hashes throughout their retention. Data shall be retained in a manner consistent with all applicable privacy laws and regulations…

Products

ArcSight; Voltage

Timing

June 4, 2021

ArcSight

Get faster, more accurate detection of known and unknown threats with a security analytics-powered SOC that intelligently adapts to talent shortages.

Voltage

Protect sensitive structured and unstructured data to reduce breach risk with privacy-enabled data usability across hybrid IT.

Solutions, Expertise, and Experience

It's all in one place.

You don't just need a piece of software. You need the solutions that will bring compliance, the expertise to run them optimally, and the experience of someone who knows the specific needs of your organization. CyberRes has everything you need to meet the eight technology mandates of the Executive Order on Improving the Nation's Cybersecurity—so you can protect, detect, and evolve your cyber resilience.

To get more information, visit our CyberRes Public Sector and Government Solutions pages. Or contact us for more information on the executive order solution.

Learn more

CyberRes