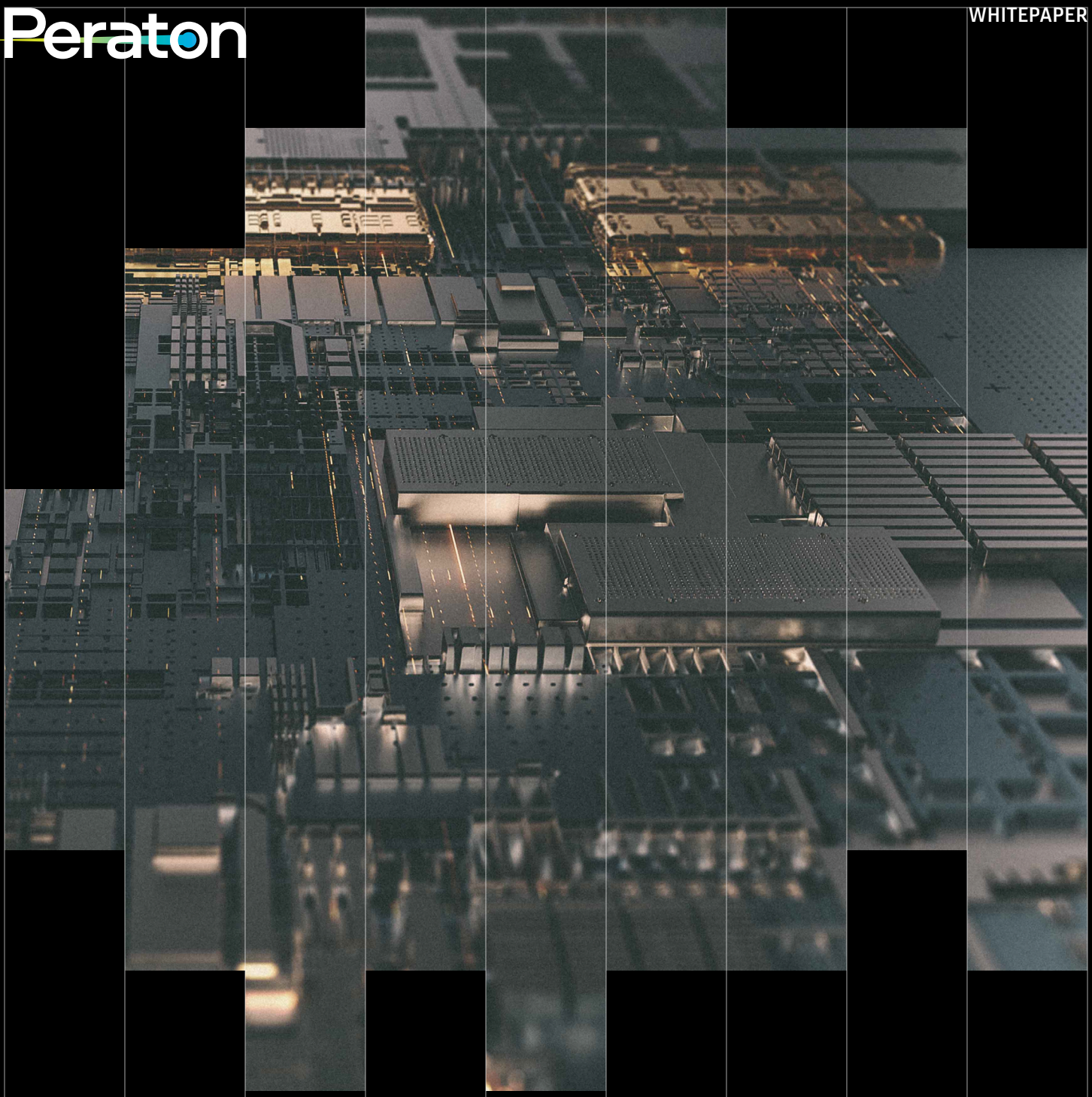
Peraton

WHITEPAPER



SUMMARY, ANALYSIS, AND SOLUTIONS FOR THE NEW EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

EXECUTIVE SUMMARY

Organizational leaders are fast discovering how digital transformation benefits their mission critical programs and business processes. Multitasking remote workers are increasingly teaming virtually, any time and from anywhere, confidently and safely leveraging efficient cloud platforms to achieve timely results. Data scientists now apply AI/ML capabilities to swiftly discern actionable trends from oceans of collected data. Technologists exploit autonomous processes to streamline previously labor-intensive tasks. Watch standers respond decisively to enterprise threats revealed in real-time on single pane displays for hyper situational awareness. These and many other welcome transformations help enable modern work environments. However, they demand high performance from the organization's cyber and information technology professionals.

Chronic shortages of expert staff, burdensome upkeep of unsafe legacy infrastructure, and overtasked program managers with little bandwidth or resources to apply to new initiatives challenge even the most dedicated teams. Additionally, the need for reliability, resilience, and security has never been greater. The audacity of sophisticated cyber actors spying on sensitive programs, disrupting business processes, or extorting fees for ransomed data increases with every successful compromise. Still, the future is bright as we are in this together. Information sharing and cooperation among partners—federal, state, local and tribal governments, the private sector, academia, as well as our international allies—will be key to our mutual success in navigating the digital road ahead.

On May 12, 2021 the Biden administration issued a new executive order (EO)[1] to enhance our nation's cybersecurity posture which notably includes coordinating partnerships with the private sector to support the EO execution. The EO represents a significant number of activities that will require directed actions and significant effort among all U.S. federal government agencies and government contractors/ subcontractors.

The new EO requirements make cybersecurity and securely managing government data more important than ever before. Peraton welcomes this opportunity to further our trusted partnership with the Federal Civilian Executive Branch (FCEB) agencies, Department of Defense (DOD), and the Intelligence Community (IC) in support of their mission accomplishment. This whitepaper highlights Peraton's capabilities that can directly enhance implementation of the EO.

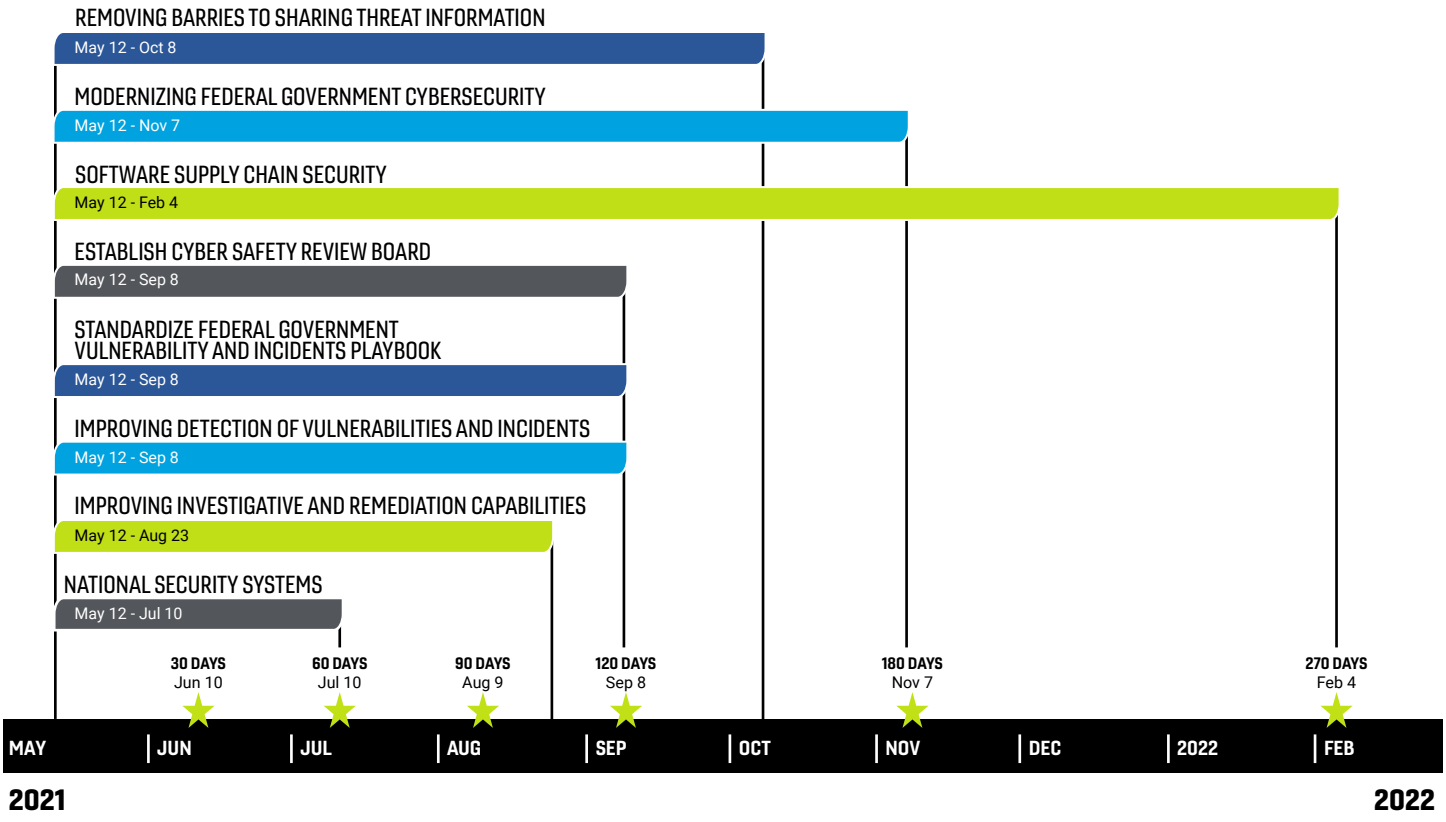
[1] Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) Presidential Actions

CYBERSECURITY EO SCOPE

The scope of the new cybersecurity EO issued by the Biden administration includes, but is not limited to the following requirements:

- Create both new and potential cyber incident reporting requirements for all information and communication technology (ICT) service providers—cloud service providers (CSPs), information service providers (ISPs), and related information technology and operational technology firms—who are U.S. federal government contractors, subcontractors, and/or supply-chain partners.
- Require all ICT service providers to promptly report all cyber incidents involving a software product or software support system used by federal government agencies within 72 hours or less of the identification of the cyber incident.
- Standardize common cybersecurity contractual requirements across federal government agencies.
- Modernize federal government cybersecurity via adopting security best practices such as including zero trust architecture (ZTA), data analytics for identifying and managing cybersecurity risks, investment in both technology and cybersecurity personnel, and secure cloud services—software as a service (SAS), infrastructure as a service (IaaS), platform as a services (PaaS).
- Ensure the Office of Management and Budget conducts an annual cybersecurity cost analysis of all new cybersecurity requirements contained in the EO.
- Modernize the current Cybersecurity Infrastructure Security Agency (CISA) cybersecurity programs to be fully functional ZTA cloud-computing environments.
- Develop a federal government cloud-security strategy.
- Ensure U.S. federal government agencies adopt agency-wide multifactor authentication (MFA) and data encryption.
- Modernize the current FedRAMP program for cloud security.
- Enhance software supply chain security.
- Create a tiered software security rating system.
- Establish a Cyber Safety Board.
- Standardize the federal government's playbook for responding to cyber vulnerabilities and incidents.
- Improve detection of cyber vulnerabilities and incidents on federal government networks.
- Enhance the federal government's cyber investigative and remediation capabilities.

EXECUTIVE ORDER (EO) TIMELINE OF ACTIONS FOR IMPROVING THE NATION'S CYBERSECURITY



The new Cybersecurity EO establishes numerous specific requirements and timelines for required actions for many federal government agencies, government contractors, and supply chain partners.

CYBERSECURITY EO KEY ISSUES AND CONCERNS

Upon careful review and analysis of the cybersecurity EO sections and specific requirements, we have identified numerous key issues and concerns. We fully recognize that many of the following issues and concerns will need to be addressed by the U.S. federal government agencies and some will require new requirements to be implemented via the Federal Acquisition Regulatory (FAR) process under the leadership of the FAR Council with input from industry over the next year or more. These include:

Removing Barriers to Sharing Threat Information

- Sharing of "vulnerabilities" information
- Definition of "potential incidents"
- Accuracy of the vulnerabilities data
- Security, storage, and access to the cyber vulnerabilities data
- Potential for cyberattacks on the shared cyber vulnerabilities database
- Enforcement penalties for noncompliance

Modernizing Federal Government Cybersecurity

- Additional funding to purchase new products and services
- Additional resources to staff the new cybersecurity programs
- Systems integration expenses and challenges with legacy IT systems
- Level of detailed requirements for ZTA
- Level of detailed requirements for cloud security
- Potential for recertification requirements for revised FedRAMP program

Software Supply Chain Security

- Lack of a standardized approach for software supply chain security
- Additional cost impact on software developers/manufacturers
- Software security liability
- Enforcement penalties for noncompliance

Establish a Cyber Safety Board

- Selection of board members
- Scope of the board's responsibilities and authority
- Board's ability to levy penalties on government contractors and supply chain partners
- Timeliness of board's actions—given the rapid rate of technology, tactics, and procedure changes by cyber threat actors

Standardize Federal Government Vulnerability and Incidents Playbook

- Need for government agency customization of cyber vulnerability and incidents playbook
- Unique missions, systems, risks, and different threat profiles of government agencies
- Additional funding and resources

Improving Detection of Vulnerabilities and Incidents

- Need for an integrated enterprise IT services management platform, including vulnerability management, integrated risk management, and incident response management
- Additional funding and resources

Improving Investigative and Remediation Capabilities

- Need for expanded cyber forensics labs and malware testing
- Need for additional cyber incident response team resources
- Need for expanded and persistent cybersecurity education, training, and simulation funding
- Competition and availability of required resources

PERATON'S CYBERSECURITY CAPABILITIES: A PATHWAY TO EXCEEDING THE NEW EO REQUIREMENTS

As the creator of the leading portfolio of cybersecurity services to support the U.S. public sector's cloud-based, on-premise, and hybrid environments, Peraton is ideally suited to address the new EO requirements and complex cybersecurity challenges. We currently manage a comprehensive portfolio of cybersecurity programs for the U.S. federal government and have the resources to support agencies in implementing enhanced cyber mission capabilities, services, and advanced solutions working with our cyber strategic partners to address all of the specific needs as outlined in the new Cybersecurity EO. The following are just a few examples of Peraton's cyber capabilities, services, and advanced solutions:

Advanced Cybersecurity Solutions (ACS)

Peraton Labs is the leading provider of advanced cybersecurity solutions and government funded cybersecurity research and development projects for the Defense Advanced Research Projects Agency (DARPA), U.S. Army Research Labs, the National Security Agency (NSA) and USCYBERCOM. Peraton Labs' 300+ communication technologists, data scientists, and software engineers have developed and deployed software to enhance malware detection, advance data forensics analysis, defend against cyber-attacks such as distributed denial of service (DDoS) attacks, protect against Zero-day cyber-attacks, and detect trojan-horse malware.

We also developed PuriFile, a data loss prevention (DLP)/content disarm and reconstruction (CDR) tool to scan/cleanse files from malware (including zero-day malware), viruses, and malicious content. PuriFile is the first DLP/CDR product certified by the U.S. Intelligence Community and heavily relied upon by the DOD.

Defensive Cyber Operations (DCO)

Peraton has developed and implemented advanced data analytics and automated playbooks for enhanced cybersecurity in partnership with ServiceNow. This significantly improves cyber vulnerability analysis, integrated risk management, and incident response capabilities.

Using Peraton's new SIFT application programmable interface (API) on the ServiceNow platform, government agencies can leverage the Tenable® vulnerability scanning and compliance information directly into the ServiceNow platform and then use new Peraton developed security orchestration and automated response (SOAR) technology to enhance the ServiceNow cybersecurity situational awareness.

To combat the increasingly sophisticated threats, Peraton developed ThreatBoard™. This technology uses a scalable and redundant cloud-based data fabric architecture that enables reduced time to recognize attacks on a broad scale by ingesting data from multiple disparate sources, regardless of size and format. Every type of data required to thwart today's cyberattacks can be consumed in real-time.

ThreatBoard can also ingest ticketing from all ticketing and security information and event management (SIEM) systems. This ability to use all data formats provides the organization with all the data required to detect, analyze, and respond to threats in a single location, thereby making it easier to correlate and make sense of the data.

Using machine learning (ML) and natural language processing (NLP), ThreatBoard highlights and selects relevant attack information from the collected data. Peraton's proprietary "Fractals"™ modular GUI front end creates a single pane of glass effect that allows every person to receive a customized view of the data and incidents based on their job role.

ZTA

Peraton has developed a zero trust methodology leveraging the NIST SP 800-207 Zero Trust Architecture design tenets to assess current government agency ZTA policies, plans, and designs and create a roadmap to an effective zero trust strategy and ZTA for the agency. We provide federal government agencies the necessary support to develop customized ZTA to meet their specific requirements—data mapping, data isolation, silicon-based isolation, data micro-segmentation, micro-perimeters, segmentation gateways, software defined perimeters, and dynamic identity verification and access control—with enhanced cyber threat intelligence, and continuous monitoring, detection, and incident response services. The Peraton ZTA methodology integrates all the related data into a security information and event management (SIEM) system such as SPLUNK or ArcSight and then further integrates the data with an information technology services management (ITSM) platform such as ServiceNow. Peraton is also weeks away from receiving an Authority to Operate (ATO) with our ZTA for one of the FCEB agencies we support.

Peraton—Cloud Services Leader

- **AWS** Migration and DevOps Competency Partner
- **AWS** Premier Consulting Partner
- **Microsoft** Gold Partner for Cloud
- **Google** GCP Partner and Government
- **VMWare** Principal Partner, and Cloud MSP
- **ServiceNow** Elite Partner

- **RedHat** Partner of the Year 2020
- **UiPath** (RPA) Partner of the year 2019
- **Peraton CloudSeed Cloud** - Washington Technology 2020 Industry Innovation Award
- **Over 50 Government** AWS and Azure government enterprise customers

Secure Cloud Services

Ranked first among federal cloud service providers for the past five years and highly recognized by our service partners, Peraton is a cloud services leader delivering the most comprehensive and secure cloud solutions and services.

Peraton works in partnership with AWS, Microsoft, Google, and IBM to offer a comprehensive suite of security services for cloud-based infrastructure and cloud-native applications, including SaaS, IaaS, and PaaS. Plus, Peraton is a certified FedRAMP Third Party Assessment Organization (3PAO). We provide continuous security compliance and protection with FITOPS and DevSecOps to create an encompassing security automation engine.

SUMMARY

The new cybersecurity EO is a comprehensive and aggressive step to improve our nation's cybersecurity posture. However, there are many specific requirements for U.S. federal government agencies, which must be funded and staffed to support and implement. There are also numerous industry cybersecurity-specific requirements which must be determined, enacted by changes and/or additions to the FAR and DFARS, funded, and contractually implemented before the actual benefits can be fully realized. As the complexity and velocity of cybersecurity challenges facing the U.S. public sector increases, Peraton is capable and ready to provide cutting edge cybersecurity services and customized solutions that support agency cybersecurity needs today and tomorrow.

Peraton

LEARN MORE AT

PERATON.COM