CYBERSECURITY EXECUTIVE ORDER TOP 10 QUESTIONS TO CONSIDER

Peraton

The following 10 questions are based upon our discussions with numerous U.S. federal government agencies CIOs, CISOs, and CTOs, government contractors, and subcontractors.

1. HOW DO WE MOTIVATE PRIVATE SECTOR FIRMS THAT PROVIDE CRITICAL MISSION SUPPORT FOR GOVERNMENT INFORMATION SYSTEMSTO SHARE CYBER INCIDENT INFORMATION IN TIMELY MANNER?

CONSIDER:

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

2. WHERE DO WE GET THE ADDITIONAL RESOURCES AND FUNDING TO PAY FOR AND MANAGE THE MANDATED MODERNIZATION OF U.S. FEDERAL GOVERNMENT CYBERSECURITY?

CONSIDER:

- Additional funding to support the purchase of new cybersecurity products and services
- Additional resources to staff the new cybersecurity programs
- Reprioritization of existing IT and cyber programs agency-wide
- Systems integration expenses and issues with legacy IT hardware, software, and related systems

3. WHAT STEPS CAN WE TAKE TO SIGNIFICANTLY ENHANCE CLOUD-BASED SECURITY ENTERPRISE-WIDE?

CONSIDER:

- Data loss/leakage
- Data privacy
- Data resilience

4. HOW CAN WE BEST ENSURE SOFTWARE SUPPLY CHAIN SECURITY?

CONSIDER:

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

5. WHAT IS THE MOST APPROPRIATE APPROACH TO IMPLEMENT ZERO TRUST CONCEPTS ACROSS THE U.S. FEDERAL GOVERNMENT AGENCIES?

CONSIDER:

- NIST SP 800-207–ZTA Design Tenets
- Micro-segmentation and segmentation gateways
- Zero trust recommended solutions based upon software defined perimeters
- Enforcement penalties for noncompliance

6. WHAT AUTHORITY AND RESPONSIBILITIES SHOULD THE NEW CYBER SAFETY REVIEW BOARD (CSRB) HAVE?

CONSIDER:

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

7. HOW SHOULD WE STANDARDIZE FEDERAL GOVERNMENT VULNERABILITY AND INCIDENT RESPONSE MANAGEMENT?

CONSIDER:

- 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

8. WHAT SPECIFIC ACTIONS SHOULD BE TAKEN ACROSS ALL U.S. FEDERAL GOVERNMENT AGENCIES TO IMPROVE CYBERATTACK DETECTION OF VULNERABILITIES AND INCIDENTS?

CONSIDER:

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

9. WHAT RESOURCES, SYSTEMS, AND TOOLS CAN WE LEVERAGE TO IMPROVE OUR CYBER INVESTIGATIVE AND REMEDIATION CAPABILITIES GOVERNMENT-WIDE?

CONSIDER:

- 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

10. WHICH CYBERSECURITY FUNCTIONS SHOULD BE OUTSOURCED TO THE PRIVATE SECTOR VERSUS MANAGING WITHIN U.S. FEDERAL GOVERNMENT AGENCIES?

CONSIDER:

- On-premise government facility versus remote contractor facility
- Staff augmentation approach versus managed security services provider
- Cost-plus-fixed-fee (CPFF) contracts versus firm-fixed-price (FFP) contracts
- Level of effort (LoE) contracts versus performance-based services contracts

CYBERSECURITY EO REQUIREMENTS AND PERATON'S CYBER CAPABILITIES, SERVICES, AND SOLUTIONS

The Presidential Cybersecurity Executive Order (EO) is a comprehensive set of new government and industry requirements designed to improve the Nation's Cybersecurity posture. As the complexity and velocity of cybersecurity challenges facing the U.S. public sector rapidly increases, Peraton is capable and ready to provide cutting edge cybersecurity services and solutions that support agency cybersecurity needs today and tomorrow.

EXECUTIVE ORDER (EO) MAJOR CYBERSECURITY REQUIREMENTS	CYBERSECURITY CAPABILITIES, SERVICES, AND SOLUTIONS
Cloud security modernization	Cloud security architecture, systems engineering, cloud migration services, and integrated solutions
FedRAMP modernization	FedRAMP 3PAO assessment and support services
Zero trust architecture (ZTA)	Zero trust assessments, policies, plans, architecture, systems engineering, and integrated solutions
Endpoint detection	Endpoint detection and response (EDR) and extended detection and response (XDR) solutions
Incident response (IR)	Enhanced incident response (IR) services integrated with security orchestration and automated response (SOAR) technology
Cyber forensic analysis	Cyber forensics analysis software and research and development (R&D) lab services
Multifactor authentication (MFA)	Advanced MFA solutions with biometrics
Software encryption	Advanced software encryption capabilities and services
Cyberattack response and remediation	Security operations center (SOC) and security information and event management (SIEM) services and solutions

ABOUT US

Peraton drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure. Peraton serves as a valued partner to essential government agencies across the intelligence, space, cyber, defense, civilian, health, and state and local markets. Every day, our 22,000 employees do the can't be done, solving the most daunting challenges facing our customers.

DO THE CAN'T BE DONE.

peraton.com

Peraton