Cyber Executive Orders & Policies

Carahsoft Policy Overview

Summary:

The United States has published policy with the intention of strengthening the country's cybersecurity posture through Supply Chain Risk Management, Zero Trust, CMMC, Critical Infrastructure Security, Cyber Incident Reporting, Continuous Diagnostics and Monitoring (CDM), Quantum Computing, and the Cyber Workforce. This overview outlines the different major pieces of policy that dictate the requirements and standards for federal agencies.

Supply Chain Risk Management		
Date	Name	Description
9/14/22	M-22-18	Memorandum for the heads of executive departments and agencies which emphasized the following: • Improve cybersecurity in critical infrastructure • Strengthen federal cybersecurity requirements • Counter ransomware attacks • Build the nation's cyber workforce • Increase international collaboration in cybersecurity Develop the National Quantum Initiative
8/22	Securing the Software Supply Chain	Document written by the NSA, CISA, and ODNI which gives guidance on how developers can secure their network
2/24/22	Securing Defense Critical Supply Chains	Document published by the Department of Defense (DoD) Identified supply chains the DoD considers critical to their mission
2/3/22	NIST SP 800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	NIST released a set of recommendations, in response to Executive Order 14028, aimed at mitigating the risk posed by software vulnerabilities. The publication outlines practices that will help software producers minimize risk.The SSDF helps organizations meet the following secure software development recommendations: • Organizations should ensure that their people, processes, and technology are prepared to perform secure software development. • Organizations should protect all components of their software from tampering and unauthorized access. • Organizations should produce well-secured software with minimal security vulnerabilities in its releases.

		• Organizations should identify residual vulnerabilities in their software releases and respond appropriately to address those vulnerabilities and prevent similar ones from occurring in the future.
2/24/21	EO 14017: Executive Order on America's Supply Chains	Executive Order on America's Supply Chains calls for: • Secretary of Commerce will begin identifying risks in the US semiconductor supply chain • Commerce and DHS will review America's Information and Communication Technology (ICT) supply chains
Zero Trust		
Date	Name	Description
06/13/2023	BOD 23-02	CISA released BOD 23-02 on June 13, 2023. This directive requires federal agencies either remove interfaces in the scope of the directive from the internet by making it only accessible from an internal enterprise network or deploy capabilities, as a part of a Zero Trust Architecture, that enforce access control to the interface through a policy enforcement point separate from the interface itself. Interfaces in the scope of the directive include: • Devices residing on or supporting federal information systems and/or networks that belong to one of the following classes: routers, switches, firewalls, VPN concentrators, proxies, load balancers, and out of band server management interfaces (such as iLo and iDRAC). • Devices for which the management interfaces are using network protocols for remote management over public internet
1/10/23	NIST SP 800-217	Document defines the requirements and characteristics of government-wide interoperable identity credentials used by federal employees and contractors.
1/10/23	NIST SP 800-157r1	Document provides technical guidelines for the implementation of reliable credentials that are issued by federal agencies to individuals who possess and prove control of their valid PIV cards.

10/21/22	DoD ZTA Strategy	DoD is working towards meeting the following objectives:
		• Zero Trust Cultural Adoption
		  ○ Cybersecurity-minded culture and workforce that embraces Zero Trust
		• DoD Information Systems Secured and Defended
		  ○ Secured communications at all operational levels a
		• Technology Acceleration
		  ○ Continually updated and advanced Zero Trust enabled IT
		• Zero Trust Enablement
		
		Enhanced operations and support performance

7/22/22	M-22-16	This memorandum outlines cyber investment priorities for FY24 budget submissions. The following areas are considered investment priorities: Zero Trust implementation, IT modernization, Risk Management, infrastructure investments, and human capital.
1/26/2022	M-22-09: Moving the US Government Toward Zero Trust	**2/25/22:** Agencies must designate zero trust strategy implementation lead **3/27/22:** • Agencies must build upon plans developed under EO 14028,

	Cybersecurity Principles	• Submit an implementation plan for FY22 – FY24 to OMB and CISA • Submit a budget estimate for FY24 **9/30/24:** Agencies must achieve specific zero trust security goals by end of FY24 related to the five pillars of Zero Trust as developed by CISA: Identity, Devices, Networks, Applications and Workloads, and Data.
1/24/22	FIPS 201-3	Document written by the Department of Commerce which establishes a standard for a Personal Identity Verification (PIV) and provides guidance for implementation and use.
1/19/22	NSM-8	This memorandum built on the guidance of EO 14028 and required all National Security Systems to comply with EO 14028 regulations. This memo also gave further clarification on EO 14028's provisions.
5/12/2021	EO 14028: Executive Order on Improving the Nation's Cybersecurity	**All deadlines have passed** The Executive Order on Improving the Nation's Cybersecurity requires agencies to: • Prioritize adoption of cloud technology, develop a plan to implement Zero Trust Architecture, and provide a report to OMB with plans detailing cloud and Zero Trust adoption • Report to CISA and OMB on types and sensitivity of agency unclassified data Report to CISA, OMB, and APNSA on progress in adopting MFA and encryption of data at rest and in transit or provide a written rationale as to why they were unable to adopt
8/11/2020	NIST SP 800-207	Introduces what NIST considers to be a Zero Trust Architecture and describes the various use cases and approaches organizations can use to implement a Zero Trust Architecture.

CMMC		
Date	Name	Description
12/30/22	DFARS 252.204-7021	Establishes the following requirements • Contractors and sub-contractors must have a current CMMC certificate level at the level required level for the duration of the contractors
12/30/22	DFARS 252.204-7020	Establishes the DoD Assessment requirements for contractor implementation of NIST SP 800-171
2/2021	NIST SP 800-172	Provides updates on previous guidance to the protection of Controlled Unclassified Information (CUI) and covers the following: • Development approach • Organization and structure • Flexible application • Requirements for CUI
12/31/2020	DODI 5000.90	DODI for Cybersecurity for Acquisition Decision Authorities and Program Managers establishes the following: • Policy • Assigns responsibilities • Prescribes procedures for the management of cybersecurity risk in the DoD
3/6/2020	DODI 5200.48	DODI for Controlled Unclassified Information (CUI) establishes the following: • Policy • Assigns responsibilities • Prescribes procedure for Controlled Unclassified Information throughout the DoD
2/2020	NIST SP 800-171	Provides guidance on the protection of Controlled Unclassified Information (CUI) and covers the following: • Basic assumptions & Development of security requirement

Critical Infrastructure Security		
Date	Name	Description
11/2/2022	NIST – Securing Water and Wastewater Utilities	NIST is seeking feedback on a proposed project to address cyber risks related to the water and wastewater sector • Aim to produce a NIST Cybersecurity Practice Guide to secure production environments
10/27/2022	FCC 22-82	FCC Proposed Action to Strengthen the Security of the Nation's Emergency Alert Systems • Requires Emergency Alert System participants, such as broadcasters and cable providers, to report incidents of unauthorized access to their Emergency Alert System equipment to the Commission within 72 hours • requiring Emergency Alert System participants and the wireless providers that deliver Wireless Emergency Alerts to annually certify that they have a cybersecurity risk management plan and implement sufficient security measures for their alerting systems • requiring participating wireless providers to transmit sufficient authentication information to ensure that only valid alerts are displayed on consumer devices
10/3/2022	BOD 23-01	• The directive, in response to the SolarWinds cyberattack, requires Federal Civilian and Executive Branch (FCEB) agencies: • Perform automated asset discovery every seven days • Initiate vulnerability enumeration on all assets every fourteen days • Apply automated upload of vulnerability enumeration results to the CDM Agency dashboard within seventy-two hours of completion • Maintain capability to perform on-demand vulnerability discovery and enumeration within seventy-two hours of CISA's request and make results available within seven days of the request While BOD 23-01 only applies to FCEB, CISA recommends that all organizations implement the guidance to protect critical infrastructure from exploitation of unknown or under protected weaknesses.

10/2022	CISA's Cross-Sector Cybersecurity Performance Goals	• CISA released a set of thirty-seven cross-sector cybersecurity performance goals (CPG) broken down into eight categories in October 2022.
		• The eight categories cover:
		  • Account security
		  • Device security
		  • Data security
		  • Governance and training
		  • Vulnerability management
		  • Supply chain / third party
		  • Response and recovery
		  • And other
		• The CPGs are voluntary, but highly recommended cybersecurity practices related to IT and operational technology (OT) for critical infrastructure owners and operators to implement.
		• Each critical infrastructure sector has different levels of cybersecurity implementations. CISA released the CPGs to establish a baseline for underdeveloped cybersecurity within critical infrastructure.

3/15/2022	H.R. 2471: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)	• CIRCIA originated as a response to the SolarWinds cyberattack in 2020. • The CIRCIA requires critical infrastructure cyberattacks be reported to CISA within 72 hours and ransomware payment within 24 hours. • The Cybersecurity and Infrastructure Security Agency issued a Request for Information (RFI) on September 12, 2022 requesting input while developing the proposed regulations required by CIRCIA.

7/28/2021	NSM-X: National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems	Released on July 28, 2021, NSM-X established **the Industrial Control Systems Cybersecurity Initiative**, a voluntary effort between the Federal Government and critical infrastructure
		  • The goal is to expand the deployment of technologies that provide **threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control system and operational technology networks** across critical infrastructure
		  • Efforts stated with the Electricity subsector then led to natural gas pipelines, water and wastewater, and chemical sectors
		Tasks DHS, and NIST with creating Critical Infrastructure Cybersecurity Performance Goals

Cyber Incident Reporting		
Date	Name	Description
6/21/2022	S. 2520: The State and Local Government Cybersecurity Act of 2021	• This law amends the Homeland Security Act of 2002, requiring the Department of Homeland Security (DHS) to share information with SLTT governments. • The purpose is to prevent cyberattack through fostering communication between the SLTT and federal resources. CISA shall provide operational and timely assistance, share threat indicators and defensive measures, notify incidents, create a platform for best practices, and educate SLTT on cybersecurity policies and procedures. CISA's relationship with the Multi-State Information Sharing Analysis Center, an organization made up of all 56 states and territories, capitals, fusion centers, and other local governments and organizations, is now required by law.
9/2/2020	BOD 20-01	• BOD 20-01 is a directive published by CISA in September 2020. • BOD 20-01 requires agencies list a security contact in charge of a .gov domain on the domain, publish a comprehensive vulnerability disclosure policy on its main website, and have a fully implemented vulnerability disclosure program. The new Vulnerability Disclosure Policy platform was announced on January 24, 2022.
Continuous Diagnostics and Mitigation (CDM)		
Date	Name	Description

12/2/2022	M-23-03: FISMA Guidance	Agencies must:
		• Automate Reporting
		  • Agencies are required to report at least 80 percent of Government-furnished equipment (GFE) through the CDM program.
		  • The core asset/device visibility tool for CDM today is Forescout
		  • The core Vulnerability Detection tool for CDM today is Tenable
		  • Starting in the first quarter of FY 2023, agencies must provide data on assets in an automated manner to the maximum extent feasible
		  • CISA and the CISO Council FISMA Metrics Subcommittee will work with OMB to identify future metrics for automation in FY 2024 and beyond
		• Acquire Capabilities
		  • Although agencies may acquire continuous monitoring tools through means other than current or future CDM acquisition vehicles, agencies must provide sufficient justification before pursuing acquisition tools not aligned with the CDM program
		• Resource Allocations
		  • When the CDM PMO procures cybersecurity tools on behalf of an agency to fulfill specific CDM requirements, the PMO will cover the license and maintenance costs of the base year and the maintenance cost for the first option year. Otherwise, CFO Act agencies are responsible for the operations and maintenance costs (e.g., licensing costs) of their CDM-related tools and capabilities. Each agency shall, in coordination with its RMO, build CDM

		requirements into budget plans in future years. For non-CFO Act agencies that are unable to pay for CDM, the CDM PMO will cover all costs • CISA should provide agencies with a list of software categories that meet the "critical software" definition no later than January 15th • CISA should provide OMB with information regarding scanning cadence and other performance data beginning in the third quarter of FY 2023 and work with OMB and the CISO Council FISMA Metrics Subcommittee to "identify future metrics for automation in FY 2024"
10/08/2021	M-22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities	Agencies must: • Review and update agency internal vulnerability management procedures • Remediate each vulnerability according to timelines set forth in the CISA-managed vulnerability catalog • Report on the status of vulnerabilities listed in the repository CISA will update and maintain vulnerability catalog
Quantum Computing		
Date	Name	Description
08/09/2023	EO 14105: Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern	President Biden signed on August 9th an Executive Order on addressing US investments in certain national security technologies and products in countries of concern. • Countries of concern include People's Republic of China (PRC), including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau. • The three sectors of sensitive technologies Treasury will regulate are semiconductors and microelectronics, quantum information technology, and artificial intelligence.
12/21/2022	H.R. 7535 – Quantum Computing Cybersecurity Preparedness Act	The OMB must submit a report to Congress on: • a strategy to address the risk posed by the vulnerabilities of information technology of executive agencies to weakened encryption due to the potential and possible capability of a quantum computer to breach such encryption; • the funding needed by executive agencies to secure such information technology from the risk posed by an adversary of the United States using a quantum computer to breach the encryption; and • a description of federal civilian executive branch coordination efforts led by NIST, including timelines, to develop standards for post-quantum cryptography. Each executive department, military department, government corporation, other establishment in the executive branch of the Government, or any independent regulatory agency must establish a current inventory of IT in use that is vulnerable to decryption by quantum computers.
11/18/2022	M-23-02: Memorandum on Migrating to Post-Quantum Cryptography	The OMB released M-23-02 on November 18, 2022. The memorandum builds off of NSM-10 and directs federal agencies to prepare for implementing post-quantum cryptography (PQC). Further, it provides transitional guidance to agencies in the period before PQC standards are finalized by the National Institute of Standards and Technology (NIST), after which OMB will issue further guidance. Deadlines outlined in the memorandum include: • **Within 30 days of publication**, all agencies shall designate cryptographic inventory and migration lead.

		• **Within 90 days of publication,** the ONDC shall release instructions for the collection and transmission of inventory and release instructions for funding assessments. • **Within 180 days of publication,** NIST shall establish a mechanism to enable the exchange of PQC testing information and best practices. • **Within 1 year of publication,** CISA shall release strategy on automated tooling and support for the assessment of agency progress towards adoption of PQC. • **By May 4, 2023 and annually thereafter,** all agencies except the Department of Defense and agencies in the Intelligence Community shall submit cryptographic system inventory • **30 days after submission of cryptographic system inventories and annually thereafter,** all agencies except the Department of Defense and agencies in the Intelligence Community shall submit funding assessments. • **Ongoing,** all agencies shall report testing of pre-standardized PQC
05/04/2022	EO 14073: Executive Order on Enhancing the National Quantum Initiative Advisory Committee	EO 14073 establishes the National Quantum Initiative Advisory Committee to help oversee the National Quantum Initiative. The Committee will: • Respond to requests from the President or the Co-Chairs of the Committee for information, analysis, evaluation, or advice relating to QIS and its technology applications • Solicit information and ideas from a broad range of stakeholders on QIS, including the research community, the private sector, academia, national laboratories, agencies, State and local governments, foundations, and nonprofit organizations • Review the national strategy for Quantum Information Science (QIS) • Respond to requests from the Subcommittees
05/04/2022	NSM-10: National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems	This NSM-10 identifies the cybersecurity risks associated with the rise of cryptanalytically relevant quantum computers (CRQC). The largest requirement of this memorandum is the full transition of all cryptographic systems to a quantum-resistant standard by 2035. The White House established the following goals: • NIST will open a working group with industry to advance the adoption of quantum-resistant cryptography and establish a Migration to "Post-Quantum Cryptography Project" at the National Cybersecurity Center of Excellence • CISA will engage state, local, and tribal government to explain risks posed by quantum computers • OMB, CISA, NIST, the National Cyber Director, and NSA will establish requirements for inventorying all currently deployed cryptographic systems, excluding National Security Systems (NSS) • The heads of all civilian agencies will provide to CISA and the National Cyber Director an inventory of their IT systems that remain vulnerable to CRQCs • The National Cyber Director will deliver a status report to the APNSA and the Director of OMB on progress made by FCEB Agencies on their migration of non-NSS IT systems to quantum-resistant cryptography.

		• The Department of Commerce will release a proposed timeline for the deprecation of quantum-vulnerable cryptography in standards • OMB will issue a policy memorandum requiring FCEB Agencies to develop a plan to upgrade their non-NSS IT systems to quantum-resistant cryptography. • Until the release of NIST algorithms, civilian agencies shall not procure any commercial quantum-resistant cryptographic solutions for use in IT systems supporting enterprise and mission operations. • The NSA shall provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS. • Agencies operating NSS shall identify and document all instances where quantum-vulnerable cryptography is used by NSS and shall provide this information to the National Manager. • Agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges, where appropriate and in consultation with the National Manager. • DOD shall deliver to the APNSA and the Director of OMB an assessment of the risks of quantum computing to the defense industrial base and to defense supply chains, along with a plan to engage with key commercial entities to upgrade their IT systems to achieve quantum resistance.
Cyber Workforce		
Date	Name	Description
07/31/2023	National Cyber Workforce and Education Strategy	The White House released its Cyber Workforce and Education Strategy on July 31st. Accomplishing the goals in this strategy requires assistance from private industry to provide education opportunities and training programs to develop the cyber workforce. The four pillars of the EO are: • Equip every American with foundational cyber skills • Transform cyber education • Expand and enhance America's cyber workforce • Strengthen the federal cyber workforce