



Next Generation Protection: Electronic Security Systems for U.S. Data Centers & Government Facilities

A Post-Productivity Era Transformation

February 2026

Executive Summary

The United States is entering a period in which the availability, integrity, and resilience of data centers and high-value government facilities will directly shape economic competitiveness and national security. Generative AI and high-performance computing are accelerating demand for dense, energy-intensive infrastructure and increasing the strategic value of these facilities that host critical data and compute. The U.S. Department of Energy has assessed that electricity demand from data centers is rising, and the 2024 United States Data Center Energy Usage Report describes how AI-accelerated servers and associated cooling and power requirements are reshaping the sector's operating profile. The International Energy Agency similarly frames AI and data centers as significant drivers of future energy demand and infrastructure planning [1].

This shift is occurring amid an expanding cyber-attack threat surface. Modern facilities depend on a dense fabric of interconnected security devices: cameras, door controllers and electronic locks, badge readers, motion sensors, fire panels, environmental monitors, and building-automation components. Many of these devices are "IoT-like" systems: embedded, network-connected, and frequently managed through vendor ecosystems. When deployed without strong cyber hygiene, they create a dual risk: physical attackers and cyber-attack groups can compromise devices to disrupt operations, tamper signals, or use devices as footholds into enterprise networks.

U.S. Federal government direction is converging on two imperatives: (1) the real and present need to enhance cybersecurity requirements for connected devices and (2) the growing need for quantum-resilient cryptography. The U.S. Congress has directed U.S. Federal government agencies to establish and apply new cybersecurity standards for Internet of Things (IoT) devices via the IoT Cybersecurity Improvement Act of 2020. NIST has provided an IoT device cybersecurity capability core baseline and acquisition guidance to operationalize these requirements (NISTIR 8259A; NIST SP 800-213). In parallel, the Office of Management and Budget (OMB) has issued U.S. Federal government direction for migration to post-quantum cryptography (PQC), and NIST has finalized initial PQC standards including the Federal Information Processing Standards (FIPS) 203 [2].

This whitepaper proposes a next generation for electronic security systems (ESS) to be elevated to an integrated security systems (ISS) model that enhances and integrates electronic wireless security, secure IoT device technology, cybersecurity engineering and operations, enterprise quantum security, and automated continuous monitoring and control. It is intended to support acquisition planning, enterprise architecture decisions, and modernization roadmaps for U.S. data centers and U.S. Government facilities.





Strategic Context: Why Facility Security Must Modernize Now

Facility security historically prioritized physical threats such as unauthorized entry, theft, sabotage, and life-safety events. Those risks remain, but the digitalization of building and security systems has created a blended threat environment in which cyber compromise can drive physical outcomes, and physical access can enable cyber compromise. For data centers, the operational consequences are outsized: disruptions can propagate into public services, financial systems, defense missions, and AI-enabled workflows that depend on continuous compute availability.

The AI era increases stakes in three ways. First, computing infrastructure is becoming more concentrated in high-value sites, increasing the attractiveness of data centers as strategic targets. Second, compute loads drive higher power density and more complex mechanical and electrical ecosystems, increasing operational sensitivity. Third, AI adoption is increasing the volume and sensitivity of data stored and processed in these environments, raising the impact of confidentiality breaches and “harvest now, decrypt later” risk addressed through PQC migration [3].

Threat Landscape: Representative Cyber-Physical Attack Scenarios

Security programs should assume adversaries will exploit the weakest pathway into a facility’s control surface. The scenarios below are representative patterns seen across modern infrastructures.

Compromise of an internet-exposed device management plane (camera, access controller gateway, or monitoring dashboard), enabling remote control or credential theft.

Pivot through a poorly segmented security device network into enterprise services, using default credentials or unpatched vulnerabilities.

Supply chain compromise of firmware or third-party software components, introducing backdoors into security devices or their management ecosystems.

Insider misuse of privileged access to disable alarms, alter access rules, or suppress video evidence, facilitated by weak role-based controls or poor audit logging.

Crypto obsolescence risk: long-lived devices relying on legacy public-key algorithms that become non-compliant during PQC transition windows, forcing emergency replacement or creating persistent exposure.



Electronic Security System (ESS): Challenges in the Current State

Legacy deployment models and labor-intensive integration

Many deployments still reflect older paradigms: dedicated wiring runs to every sensor and controller, proprietary protocols and management platforms, and integration through custom interfaces. This approach can be reliable, but it becomes slow and expensive to extend, particularly in retrofit environments and multi-building campuses. In high-density data centers, physical change must be coordinated with availability requirements and power/cooling constraints, making hand integration a schedule driver.

Legacy architectures often separate “facility security” from “cybersecurity,” with distinct integrators, networks, and monitoring tools. This separation reduces accountability for end-to-end risk outcomes, such as whether controllers are patched, whether management planes use strong authentication, and whether consoles produce auditable evidence for compliance and incident response.

Insecure IoT devices and weak lifecycle management

Security and facility devices increasingly share common IoT risk patterns: embedded operating systems, remote management services, cloud connectors, and dependencies on third-party software. When devices lack secure defaults, strong credentialing, vulnerability disclosure processes, and supported patch lifecycles, they become high-risk infrastructure. NISTIR 8259A defines a device cybersecurity capability core baseline that can be used to define measurable expectations for device fleets [4]. NIST SP 800-213 provides a risk-managed framework for building IoT device requirements into acquisition and system design [5].



Limited automated monitoring, response, and evidence generation

Many environments lack automated correlation and response workflows that connect physical security events to Security Operation Centers (SOCs) operations and incident response. Uptime Institute’s outage analysis underscores that incidents and outages remain material risks for digital infrastructure environments, and that operational factors continue to influence failure outcomes [6].

NIST’s guidance emphasizes ongoing awareness of security status and supports risk decisions through continuous monitoring data and governance [7]. Extending Information Security Continuous Monitoring (ISCM) concepts to cyber-physical systems is essential for portfolio-scale audit readiness, control verification, and operational resilience.

Limited quantum preparedness and crypto agility gaps

Facility systems often have long lifecycles. When controllers, panels, or management platforms embed cryptographic libraries that will need PQC updates, the migration burden accumulates silently. OMB directs agencies to inventory systems using public-key cryptography and plan migration [8]. NIST’s finalized PQC standards provide a standards-based foundation for migration planning [9]. Absent explicit requirements for crypto agility and PQC readiness, organizations risk acquiring systems that are expensive or impossible to modernize later.

Next Generation: Integrated Security Systems (ISS)

A next-generation approach treats electronic security as an enterprise platform: interoperable components secured and monitored like mission IT. The model below is organized around five integrated capability pillars.

Wireless and hybrid connectivity for agile deployment

Wireless technology can reduce time-to-deploy for certain sensors and coverage areas, support temporary or surge requirements, and improve flexibility in retrofit facilities. Because radio access is easier to reach than physically isolated wiring, wireless segments must be engineered with strong authentication, encryption, and monitoring. NIST's WLAN guidance emphasizes lifecycle security configuration and monitoring [10]. A pragmatic model is hybrid: use wired where availability and bandwidth requirements are strict and use wireless where it provides a clear operational benefit and can be continuously monitored.

Secure IoT device technology and procurement baselines

Securing connected IoT devices begins before purchasing. Programs should define minimum device security capabilities, vendor support expectations, and verification mechanisms. NISTIR 8259A and NIST SP 800-213 provide a practical basis for device requirements and acquisition language [11]. For security devices, minimum expectations should include unique device identity; support for strong authentication and role-based access; protected interfaces; secure update mechanisms; security-relevant logging; and defined product support periods.



Integrated Cybersecurity Systems: Zero Trust and Modern Identity (HSPD-12)

Zero trust architecture (ZTA) principles apply directly to cyber-physical systems: do not trust devices or individuals simply because they are “inside the building,” but instead continuously validate identity and posture and enforce least privilege at every boundary. NIST SP 800-207 defines these zero trust concepts and components, which the ISS model operationalizes by integrating the core tenets of Homeland Security Presidential Directive 12 [12]. While HSPD-12 established the mandate for common, reliable identification standards for all U.S. Federal employees and contractors, NIST FIPS 201-3 provides the modernized technical specifications for Personal Identity Verification (PIV) systems required to meet today’s security challenges.

The ISS approach evolves this framework from a static, card-based check to a dynamic Identity, Credential, and Access Management (ICAM) strategy as outlined in OMB M-19-17. In practice, this implies segmentation by device class, policy enforcement protecting management planes, and continuous verification using telemetry such as firmware version, configuration drift, and behavioral anomalies. By leveraging PIV and derived credentials as defined in FIPS 201-3 as the primary root of trust, the ISS framework bridges the gap between physical and logical security. This ensures that access to high-value data centers is governed by continuous, risk-adaptive authentication and privileged access management, aligning with the Department of War’s recently released zero trust architecture for Operational Technology (OT) environments. Furthermore, as agencies migrate to Post-Quantum Cryptography (PQC), the ISS model ensures that the underlying Public Key Infrastructure (PKI) supporting HSPD-12 and FIPS 201-3 remains resilient against emerging quantum threats.

Enterprise quantum security system: PQC readiness and crypto agility

Enterprise quantum security should be approached as a risk-managed transition. OMB direction begins with crypto inventory and prioritization [13]. NIST’s finalized PQC standards provide a standards-based foundation for migration [14]. For electronic security systems, PQC readiness includes cryptographic inventories for device fleets and management systems, upgrade/replace plans for non-updatable components, and procurement language mandating crypto agility and vendor roadmaps.

Integrated and automated continuous monitoring and control

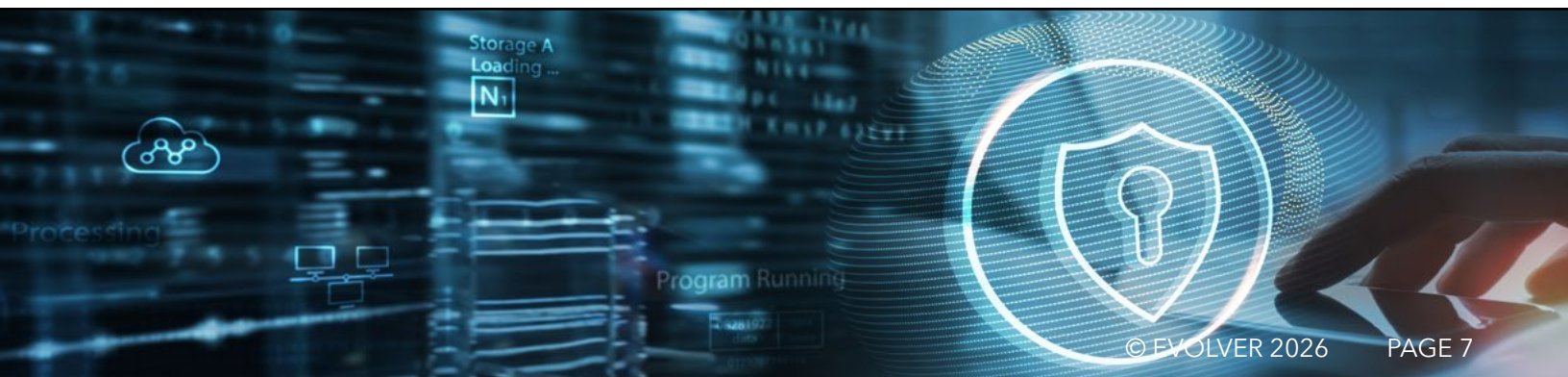
Next generation security systems should provide a unified operational picture that integrates physical security events with cyber telemetry. NIST SP 800-137 outlines an ISCM approach that maintains ongoing awareness of vulnerabilities and threats [15]. In practice, organizations should (a) ingest device inventories and vulnerability data, (b) collect security-relevant logs from management platforms and administrative endpoints, (c) normalize events for correlation, and (d) automate response actions with human governance. Over time, this enables portfolio-scale analytics on trends such as recurring alarm patterns, patch compliance, and the relationship between physical and cyber anomalies.

Integrated Security System (ISS): A Five-Layer Model Reference Architecture

Programs can standardize a reference architecture to clarify control points and responsibilities across a facility portfolio. The model below supports repeatable deployment patterns, consistent control enforcement, and measurable compliance. It also clarifies where integrators must provide artifacts to support assessment and authorization, and continuous monitoring.

Layer	Representative Components	Security Requirements (Example)
Device	Cameras, controllers, locks, sensors, panels; gateways/edge	Unique identity; secure configuration; secure update; logging (NISTIR 8259A).
Connectivity	Wired + wireless; segmentation/Software Defined Network (SDN)	Strong authentication & encryption; micro segmentation; monitoring (NIST SP 800-153).
Identity & Trust	Personal Identity Verification (PIV) integration; Identity Access Management (IAM) /Public Key Identity (PKI); privileged access management	Least privilege access; governed credentials; PQC planning (OMB M-23-02).
Monitoring & Response	PACS/Vulnerability Management System (VMS)/Intrusion Detection System (IDS) consoles; Security Information & Event Management (SIEM)/Security Orchestration & Automated Response (SOAR) integration	Correlation; playbooks; audit trails; ISCM alignment (NIST SP 800-137).
Governance	Policies; baselines; Authorization & Assessment artifacts; metrics	Control alignment; continuous evidence; resilience reporting (NIST SP 800-53 Rev. 5).

Table 1. Reference architecture layers and representative requirements.



Engineering Practices That Make Integration Real

Technology modernization fails when programs treat “integration” as an interface exercise rather than an engineering discipline. The practices below enable scale and measurable risk reduction.

Network and management-plane protection

Isolate security device traffic into dedicated segments, protect management interfaces behind strong authentication and privileged access workflows, and enforce least privilege access (LPA) for service accounts. Avoid flat networks where a compromised device can reach enterprise identity services or monitoring infrastructure.

Configuration baselines and patch discipline

Define golden configurations for each device class and management system, monitor drift, and maintain an authoritative inventory. Require vendors to provide patch cadence expectations and emergency patch procedures. For devices that cannot be patched, implement compensating controls and planned replacement timelines.

Logging, telemetry, and correlation

Collect security-relevant logs from management platforms, controllers, and authentication components. Normalize event data so that badge events, door state changes, and video analytics can be correlated with cyber telemetry. This enables faster triage and reduces nuisance alarms through corroboration.

Resilience and fail-safe design

Define how systems behave during network loss, power events, and cyber containment actions. Ensure that life-safety functions remain operable, and that security does not depend on a single cloud dependency without continuity planning. Resilience engineering should include tabletop exercises and testing of degraded-mode operations.

Benefits of Next Generation Technology

- Faster incident detection and validation by correlating physical events with cyber telemetry, reducing false positives, and improving confidence.
- Faster response through automated, governed playbooks that can isolate devices, revoke credentials, and trigger operational workflows.
- Reduced cyber-attack risk by enforcing secure IoT baselines, strong identity, segmentation, and lifecycle patching.
- Improved evidence generation for A&A and continuous compliance via inventories, baselines, patch status, and audit-ready logs [16].
- Quantum readiness through crypto inventory and standards-based PQC transition planning aligned to federal direction [17].



Metrics and Governance: What Executives Should Ask For

Executives and program leaders can improve accountability by requiring clear, measurable outcomes. The table below illustrates portfolio-level metrics that connect operational performance to risk management.

Metric	What it Indicates	Example Target
Device inventory completeness	Whether all security devices are known and managed	$\geq 98\%$ of devices inventoried
Patch compliance (critical)	Exposure to known vulnerabilities across device fleets	$\geq 95\%$ patched within Service Level Agreement (SLA)
Configuration compliance	Drift from approved baselines	$\geq 95\%$ compliant
Mean time to detect (MTTD)	Speed of detecting validated incidents	Trend downward quarter-over-quarter
Mean time to respond (MTTR)	Speed of containment and response	Defined by incident tier
PQC readiness coverage	Progress toward crypto inventory and PQC migration	100% inventory; prioritized plan

Table 2. Example metrics to govern cyber-physical security programs.



Implementation Roadmap (Portfolio View)

Phase 0 (0-60 days)

Governance and Baselines

- Stand up a cross-functional steering team (physical, facilities/OT, CISO/SOC, EA, acquisition).
- Define reference architecture and minimum baselines for devices, networks, identity, logging, and patching.
- Adopt IoT acquisition requirements aligned to NIST SP 800-213 / 8259A and the IoT Cybersecurity Improvement Act.
- Begin crypto inventory and PQC readiness assessment aligned to OMB M-23-02.

Phase 1 (60-180 days)

Inventory, Segmentation, Monitoring Uplift

- Complete device inventories and identify unsupported components.
- Implement segmentation and secure remote administration for device management plans.
- Integrate events/logs into SIEM; establish correlation rules and initial response playbooks.
- Operationalize patching and configuration management for device fleets.

Phase 2 (6-18 months)

Modernize Devices and Integration

- Upgrade/replace devices that cannot meet baseline requirements.
- Normalize events across PACS/VMS/IDS; scale workflows and evidence generation.
- Pilot PQC in management systems, VPNs, and certificate infrastructure; require vendor roadmaps.

Phase 3 (18-36 months)

Optimize, Automate, Validate Resilience

- Mature continuous monitoring and executive reporting.
- Conduct cyber-physical exercises and validate recovery procedures.
- Execute planned PQC transitions and verify interoperability across vendors and integrators.

Acquisition Considerations: Language That Drives Outcomes

Modernization outcomes depend on acquisition language that makes security verifiable. Programs should avoid requirements stated only as aspirations and instead require measurable capabilities and artifacts. IoT device procurement should align with the IoT Cybersecurity Improvement Act of 2020 and NIST IoT guidance [18].

Illustrative contract deliverables that support verifiable outcomes include:

Layer	Representative Components	Security Requirements (Example)
Device Inventory & CMDB Feed	Authoritative inventory with device attributes, firmware, location, owner	A&A evidence; vulnerability and lifecycle management
Configuration Baselines	Approved secure configurations per device class; drift reports	Continuous compliance; rapid recovery
Patch & Vulnerability Reports	SLA tracking and exceptions; compensating controls	Risk reporting; remediation governance
Event/Log Integration Plan	Log sources, formats, retention, correlation use cases	SOC integration; incident response
Governance	Policies; baselines; Authorization & Assessment artifacts; metrics	Control alignment; continuous evidence; resilience reporting (NIST SP 800-53 Rev. 5).

Table 3. Example deliverables to drive measurable outcomes.

Recommended acquisition constructs include:

- Minimum device security capabilities mapped to NISTIR 8259A (identity, secure configuration, protected interfaces, secure update, logging).
- Lifecycle requirements: vendor support period, patch cadence, vulnerability disclosure process, end-of-life transition support.
- Network and management-plane requirements: segmentation, privileged access management, Multi-Factor Authentication (MFA) for administration, secure remote access.
- Crypto agility and PQC: explicit vendor roadmaps and upgrade commitments aligned to OMB migration direction and NIST PQC standards [19].
- Operational validation: annual cyber-physical exercises and resilience testing with documented after-action reports.

Common Pitfalls and Mitigations

Programs can reduce schedule and cost risk by anticipating predictable failure modes in modernization efforts. The items below are common pitfalls with practical mitigations.

- Treating security devices as “out of scope” for cybersecurity: Define ownership, inventories, baselines, and patch SLAs for device fleets; integrate telemetry into SOC operations.
- Buying “feature-rich” systems without verification artifacts: Require inventories, baselines, logs, test results, and vendor roadmaps as deliverables, not implied capabilities.
- Flat networks and weak management-plane security: Implement segmentation and privileged access management for administration; enforce MFA and least privilege.
- Unplanned end-of-life and unsupported firmware: Maintain lifecycle plans and budget lines for device refresh; require vendor support periods and patch commitments.
- Over-automation without governance: Implement automation with guardrails and human approvals for high-impact actions; test playbooks regularly.
- Ignoring PQC and crypto agility: Inventory cryptography early; require crypto agility and PQC roadmaps in procurement; plan for staged migration
- Insufficient resilience testing: Exercise degraded-mode operations (network loss, power events, containment actions) and document recovery procedures.



U.S. Federal Government Alignment Considerations

NIST SP 800-53 Rev. 5 provides a common control catalog that includes physical and environmental protections as well as technical controls relevant to cyber-physical systems [20]. Programs can accelerate assessment and authorization and continuous monitoring by pre-mapping electronic security capabilities to relevant controls and by producing objective evidence (inventories, baselines, patch status, logs, incident records, and test results).

For many programs, a practical approach is to define a “security system Authority to Operate (ATO) boundary” for management platforms, supporting servers, and administrative workstations, while treating embedded devices as managed endpoints. This boundary should be explicit in system security plans, with clear ownership for configuration, patching, monitoring, and incident response responsibilities.



Summary & Conclusion

Electronic security systems for U.S. data centers and U.S. Government facilities are at an inflection point. The facilities that power AI-enabled missions and support critical public services are increasingly dependent on networked devices and software-defined platforms. This creates opportunities such as better analytics and operational integration, but also concentrates risk when devices are insecure, unpatched, or poorly segmented.

A next generation approach integrates modern electronic wireless security, secure IoT device technology, cybersecurity engineering and operations, enterprise quantum security, and automated continuous monitoring and control. By adopting a reference architecture, requiring verifiable acquisition outcomes, and executing a phased portfolio roadmap, organizations can reduce response time, improve assurance and auditability, and build a practical path to quantum-resilient cryptography aligned to federal direction [21].



About the Authors



Gregory A. Garrett is the Chief Operating Officer of Converged Security Solutions (CSS), leading expert teams within business units Evolver and eVigilant. These groups provide advanced IT, AI, cybersecurity, electronic security, and eDiscovery services to federal agencies and Fortune 500 companies.

With over 25 years of executive experience and a background as a CIO, CTO, CISO, and COO, he has managed more than \$40 billion in global tech contracts and served in key roles across both large and mid-sized firms.

A retired U.S. Air Force Colonel and accomplished author, Garrett has also contributed extensively to industry thought leadership through 24 books, more than 150 articles, expert testimony, and over 250 speaking engagements.



Billy Conner serves as President of eVigilant, where he leads the delivery of electronic security solutions. He brings more than 25 years of executive experience across physical security, cybersecurity, and infrastructure management, with a strong focus on operational excellence and customer outcomes. Conner's career draws from multiple senior leadership roles overseeing large-scale, complex security programs for government agencies and commercial enterprises. His expertise enables organizations to execute mission-critical solutions in a rapidly evolving security landscape.



Dr. Brian McElyea is an accomplished cybersecurity executive recognized for leading largescale digital transformation initiatives and building high-performing Cyber Centers of Excellence that drive mission-aligned security outcomes.

With over two decades of leadership across healthcare, defense, and federal sectors, he has guided global organizations through the complexities of risk management, compliance, and modernization with measurable results.

Works Cited

- [12] Department of Homeland Security. Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors. 27 Aug, 2024.
- [6] Donnellan, Douglas, and Andy Lawrence. "Annual Outage Analysis 2024: Executive Summary." Uptime Institute, Mar. 2024.
- [18, 21] Internet of Things Cybersecurity Improvement Act of 2020. Public Law 116-207. 4 Dec. 2020.
- [1] International Energy Agency. Energy and AI. International Energy Agency, 2025.
- [4, 11] National Institute of Standards and Technology. IoT Device Cybersecurity Capability Core Baseline. NIST Interagency Report 8259A, May 2020.
- [5, 11, 18] National Institute of Standards and Technology. IoT Device Cybersecurity Guidance for the Federal Government. NIST Special Publication 800-213, Sept. 2021.
- [7, 15, 16] National Institute of Standards and Technology. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137, Sept. 2011.
- [2, 9, 14, 17, 18, 21] National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication 203, 13 Aug. 2024.
- [20] National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Rev. 5, Sept. 2020.
- [12] National Institute of Standards and Technology. Zero Trust Architecture. NIST Special Publication 800-207, Aug. 2020.
- [1] Shehabi, Arman, et al. 2024 United States Data Center Energy Usage Report. Lawrence Berkeley National Laboratory, Dec. 2024.
- [10] Souppaya, Murugiah, and Karen Scarfone. Guidelines for Securing Wireless Local Area Networks (WLANs). NIST Special Publication 800-153, Feb. 2012.
- [1] U.S. Department of Energy. "DOE Releases New Report Evaluating Increase in Electricity Demand from Data Centers." 20 Dec. 2024.
- [2, 3, 8, 13, 17, 19, 21] Young, Shalanda D. Migrating to Post-Quantum Cryptography. Memorandum M-23-02, Office of Management and Budget, 18 Nov. 2022.