Post-Quantum Considerations for Operational Technology

Publication: October 2024
Cybersecurity and Infrastructure Security Agency

Executive Summary

- Cyber intrusions and compromises leveraging future quantum computing capabilities may threaten data confidentiality and integrity or undermine important access controls dependent on public-key cryptography.
- Operational technology (OT) platforms, networks, and environments are often less dependent on cryptography than information technology (IT) platforms but may be vulnerable to cryptanalytically relevant quantum computer (CRQC)-enabled intrusions in rare critical instances.
- OT specifically may be vulnerable due to connectivity or association with IT platforms as well as direct or indirect dependencies on public-key cryptographic features including encryption and decryption, signing and validation schemas, and identity and access management mechanisms.
- OT vendors, owners, and operators should plan for emerging CRQC capabilities and implement mitigations, including minimizing OT exposure to quantum threats via strong OT network segmentation, using quantum-resistant algorithms where appropriate, ensuring crypto-agility in applications and protocols, and applying quantum mitigation considerations to platform update schedules and upgrade lifecycles.

Background

Nation-states and private companies are actively pursuing quantum computing capabilities. Quantum computing could support significant technological advancement; however, malicious applications of this new technology include threats to the digital systems underpinning U.S. critical infrastructure. Specifically, quantum computing capabilities threaten to undermine current public-key cryptographic standards, which provide data confidentiality and integrity and support key elements of network security. While quantum computing technology capable of breaking standard public-key cryptographic algorithms does not yet exist, government and critical infrastructure entities—including both public and private sector entities—must act now to prepare for future quantum cryptographic threats.

The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) are taking steps to facilitate the eventual transition to post-quantum cryptography, as outlined in Secretary of Homeland Security Alejandro N. Mayorkas' March 2021 vision for cybersecurity resilience. This includes DHS's policy guidance and roadmap for post-quantum cryptography, as well as CISA's post-quantum initiative, which aims to drive and unify public and private sector efforts to address threats posed by quantum computing. CISA has also examined post-quantum threats to National Critical Functions (NCFs) and contributed to guidance on the migration to post-quantum cryptography. This document builds on those efforts by examining the specific risks that quantum computing could pose to industrial control systems (ICS) and other operational technology (OT). The target audience for this document is U.S. critical infrastructure owners and operators that rely on OT systems, networks, and other environments with current or future cryptographic security needs. OT vendors and manufacturers are also important stakeholders in establishing post-quantum resilience through Secure by Design and Secure by Default product security principles.

Public-Key Cryptography Basics

All secure digital communications—email, online banking, online messaging, etc.—rely on cryptographic mechanisms including encryption, signatures, and validation that are built into the devices and applications that transmit and store data. Cryptographic applications are based on mathematical functions that secure data, protecting it from tampering or espionage. The algorithms behind public-key (asymmetric) cryptography rely on cryptographic keys to encrypt data and authenticate the sender and recipient. Secure communication is often dependent on public-key cryptographic security even when stronger shared-key (symmetric) cryptography protects the bulk of data in transit.

Public-key encryption and signing require that each participant in an exchange of data have two separate but related digital keys—one public key and one private key—to protect data or verify a message's origin. The sender and recipient of the data can share their public keys without downgrading the level of cryptographic security but do not share their private keys.

The sender often uses the recipient's public key to encrypt small bits of data and the recipient uses their corresponding private key to decrypt that data. To reply, the recipient becomes the sender and follows the same procedure. Similarly, digital signatures allow a sender to sign a message with their private key and the recipient to use the sender's public key to verify the origin of the message, often accompanied by other mechanisms that preserve message integrity. It is standard practice for organizations to regularly use public-key cryptography to secure sensitive data, verify digital signatures, and protect user information online.

The Quantum Threat to Public-Key Cryptography

When quantum computers reach higher levels of computing power, speed, and error correction, they will very likely be capable of breaking the public-key cryptography algorithms that are in use today. A cryptanalytically relevant quantum computer (CRQC) will threaten the security of a wide range of operational processes and data. Quantum computers will likely require even greater sophistication and computational capability to break current symmetric (shared key) cryptography algorithms. Simpler symmetric encryption mitigations, such as extending key length, will likely be effective against CRQCs, at least for the near future.

The National Institute for Standards and Technology (NIST) is currently developing a suite of post-quantum cryptographic standards.[1] However, until organizations successfully implement these standards in their systems, U.S. digital infrastructure systems and the public-key cryptography they rely on for encryption will be vulnerable to quantum computing capabilities.

Quantum Risks to OT

The overall quantum risk to—and mitigations for—OT systems varies significantly from information technology (IT) due to differences in their respective functions, asset lifecycles, and use of encryption for security. CISA anticipates that implementing post-quantum cryptography for OT systems will be a significant and enduring challenge for owners and operators of U.S. critical infrastructure.

Though fewer OT devices and use cases rely on encryption mechanisms than IT systems, the criticality of many OT systems' operational roles and existing constraints in implementing technological change may still result in significant risks to U.S. critical infrastructure.

OT Cryptography Use Cases

Asymmetric cryptography enables some key factors of industrial operations. OT systems have significantly fewer applications of asymmetric encryption and signing than IT due, in part, to limitations imposed by legacy technology and other factors delaying digital transformation.[2] Even with these limitations, asymmetric cryptography in current-generation OT environments may authenticate devices, sign messages, validate signatures, verify software sources including during the boot process, and protect sensitive messages.

OT deployments may leverage asymmetric-key encryption, decryption, signature, or validation mechanisms in the following example cases:

- Managing virtual private network (VPN) or over-the-internet remote connectivity supporting multi-site operations or distributed networks wherein underlying OT systems may not use encryption.
- Limiting access to sensitive OT data, including OT system design, operation, connectivity, and configuration.
- Limiting access to datastores supporting compliance, efficient production, or validating safety mechanisms through historians or other databases.
- Restricting permissions for applying changes to operational processes, such as modifying ladder logic or modifying automated emergency protocols.
- Validating sources for software or firmware updates, plug-ins, add-ons, or other programs or platforms installed adjacent to OT systems or networks.
- Supporting certificate-based OT encryption or validation in protocols, such as Open Platform Communications United Architecture (OPC UA) and Modbus Transmission Control Protocol (TCP).[3,4]

Traditional asymmetric encryption often contributes to mechanisms that preserve information, grant authenticated access, and protect communications in a way that is effective against compromise from classic, pre-quantum computers. A CRQC-enabled attack against OT systems without post-quantum protections poses a threat to all such use cases, although specific risks will vary by targeted platform and organizational context.

Resulting Risks

Post-quantum risks to OT will likely vary significantly between organizations, as ICS and other OT system implementations are often unique. However, for every pre-quantum asymmetric encryption mechanism, the advent of a CRQC poses a similar threat: allowing the attacker to masquerade as trusted sources, freely tamper with information undetected, or decrypt information used to protect communication channels. The list below highlights some of the specific concerns for OT systems.

- **Unauthorized remote access**: Exploiting public-key-dependent remote access functionality may grant the attacker direct access to OT local networks, supervisory control mechanisms, or important OT interfaces.[5,6] Attackers may leverage trust between connected devices and legitimate software to cause extensive damage to critical infrastructure systems or threaten human safety.[7,8]
- **Manipulating important messages passed between devices:** Machine-in-the-middle attacks exploiting public-key protected traffic provides attackers with means to manipulate or change messages, which may contain commands or reports from one OT device to another virtually undetected.[9,10] Attackers may gain complete effective control of a subordinate OT unit, misrepresent actual system behavior to a supervising or monitoring unit, or both.[11]
- **Highly persistent malware installations:** Attackers may exploit public-key-based Secure Boot protections used to ensure integrity of core system software and firmware and defend against malware manipulating a system's basic input/output system (BIOS) activity, boot loader, or kernel.[12,13] Attackers can leverage malware undetected by Secure Boot features to create persistent, high-privilege backdoors or to execute effective follow-on attacks, including extortion attacks and destruction or theft of data.[14,15]
- **Decrypt sensitive or protected information:** Although attacks against information confidentiality are not as impactful for OT (vs. IT) communications, attackers could harvest and exfiltrate or intercept encrypted OT traffic in real time that is dependent on a measure of public-key encryption protection.[16] Attackers may be able to uncover OT or connected IT device credentials, gain additional insight into OT networks and traffic, or steal intellectual property such as proprietary control mechanisms, code, or designs.[17]

The immediate consequences for successful or even failed intrusions can be extreme, depending on the type of compromise and operational context of an exploited OT platform. In some cases, attacks may disrupt or even physically damage entire industrial, manufacturing, or other heavy equipment automation systems beyond repair, put human safety at significant risk, or both. In addition to cyber-induced disruption, the cyber and physical incident response process may itself impact operations and lead to downtime.

Even without a CRQC, a sophisticated threat actor could compromise OT systems with similar consequences. However, a CRQC could make it easier for adversaries to carry out such attacks on OT systems, including by exploiting connectivity or other pathways between IT and OT devices and networks. Given the importance of OT systems for enabling industrial operations in all critical infrastructure sectors, such disruptions could impact the provision of NCFs and other essential services.

Additional Risk Considerations

OT systems in U.S. critical infrastructure are responsible for the operations that enable many NCFs but may account for some of the last remaining platforms to achieve post-quantum cryptographic standards due to long software patching cycles, hardware replacement times, and strict procedures and governance.

- OT endpoints account for a significant proportion of out-of-date operating systems and software platforms that remain in operation, including those considered end-of-life (i.e., no longer supported by the software providers).[18,19]
- Some OT platforms or systems require extensive safety testing after software updates due to complicated process interdependencies or highly sensitive environments, including automating heavy equipment or controlling highly combustible materials.[20,21]
- For some systems, software required to perform certain tasks may only be compatible with unsupported operating systems such as Windows XP or UNIX, deprecated software libraries and functions, or proprietary, closed-source applications that are no longer available or supported by vendors.
- Safety compliance, auditing, or other validation requirements may also create situations where OT platforms are subject to significantly extended lifetimes when compared to IT.[22] Some extreme OT use cases such as nuclear power generation may require operation of decades-old but compliant, validated systems to maintain safe operation and reliable compatibility with surrounding technology.[23,24]

Recommendations

Plan for Post-Quantum Computing

The transition to post-quantum cryptography will be a complex, multi-year process. OT owners and operators cannot wait until the advent of a CRQC to develop and implement a plan. While this process will likely evolve as quantum computing capabilities improve, CISA's current understanding suggests that post-quantum algorithms available from NIST in 2024 will be resilient against CRQCs.[25,26] Many of the necessary planning steps (e.g., identifying personnel and resources, inventorying systems) can begin immediately.

DHS's post-quantum cryptography roadmap is a helpful starting point for all organizations. Given the specific characteristics of OT systems, inventorying and prioritization (steps 2 and 6 in the roadmap) will be critical steps for balancing system protection and resource requirements:

2. *Organizations should inventory the most sensitive and critical datasets that must be secured for an extended amount of time. This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.*

6. *Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:*
    1. *Is the system a high value asset based on organizational requirements?*
    2. *What is the system protecting (e.g., key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?*
    3. *What other systems does the system communicate with?*
    4. *To what extent does the system share information with federal entities?*
    5. *To what extent does the system share information with other entities outside of your organization?*

6. *Does the system support a critical infrastructure sector?*
7. *How long does the data need to be protected?*

Entities should leverage the DHS roadmap and other similar efforts to develop and implement a post-quantum transition plan specific to their organization. Tailoring transition roadmaps to OT systems may also require additional considerations, such as instances where remote access or over-the-internet communications are important or necessary, whether any encryption is feasible, the means or regularity of applying updates, or acceptable interruptions to operational tempo.

Reduce Exposure to Quantum Threats

In addition to implementing quantum-specific resilience measures, entities can leverage traditional cybersecurity practices to reduce vulnerabilities in OT systems that attackers could leverage a CRQC to exploit. Entities can meaningfully reduce the risk from quantum-related threats by employing a defense-in-depth approach that layers pre- and post-quantum protections such as access controls, intrusion detection, personnel cybersecurity training, and efficient incident response and business continuity practices to protect important IT and OT networks and devices.[27] Successfully implementing such protections may also reduce the footprint that OT owners and operators will need to apply post-quantum security protections to.

Strong OT network segmentation can be particularly effective in mitigating vulnerabilities associated with post-quantum cryptographic compromises by denying attackers access to OT systems.[28,29,30]

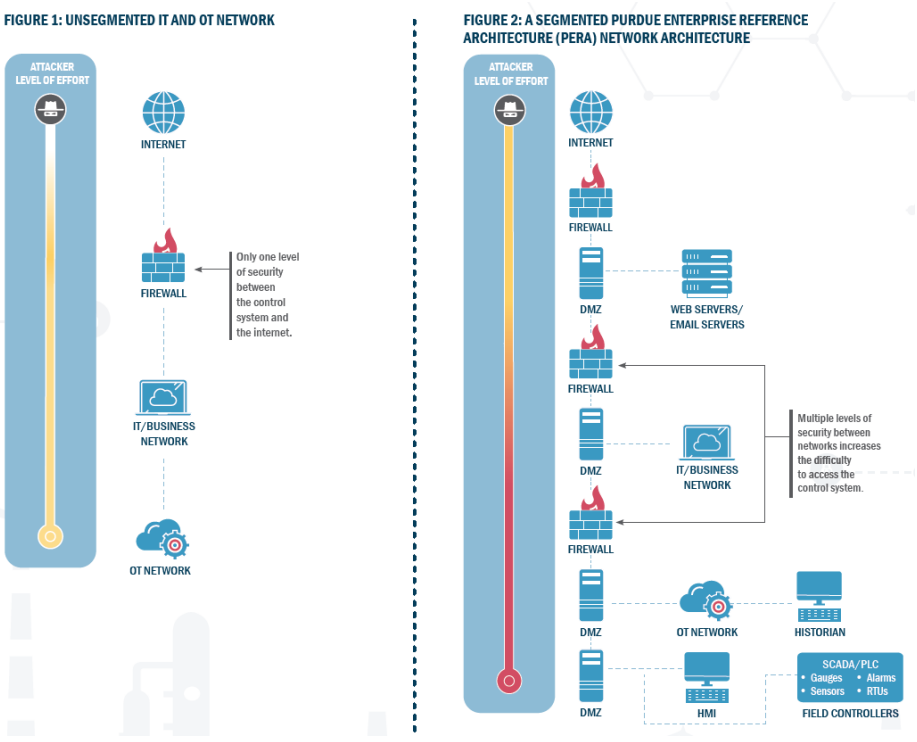

Figure 1: Network Segmentation[i]

[i] CISA, Layering Network Security Through Segmentation

Segmentation best practices include minimizing OT or OT-connected devices at the network perimeter (edge) and within or connected to an IT environment through intermediary "jump" devices, one-way transmission hardware diodes, data servers, and demilitarized zone (DMZ) segments.[31,32,33]

Strong OT network segmentation can protect OT public-key information and reduce threat actor access to connections used to manipulate OT messages, exhaust resources, and compromise OT devices. Entities should prioritize network segmentation for legacy OT, end-of-life software, and platforms that require extensive time to apply updates.[34,35,36]

Some multi-factor authentication (MFA) mechanisms can provide an additional layer of authentication without relying on pre-quantum public-key cryptography. Proper implementations of physical token or biometric identification as a second or third authentication factor may provide post-quantum protection against unauthorized access of supervisory control and data acquisition (SCADA), human-machine interface (HMI), or other OT interface platforms.[37] However, existing MFA implementations may rely on public-key cryptography for unauthorized access protection themselves or for establishing identity and access management mechanisms for an enterprise.[38] These platforms are vulnerable to CRQC intrusions until updated or replaced with post-quantum protections.

Build in Crypto-Agility

Crypto-agile platforms, including operating systems and compatible software with strong vendor support, give OT owners and operators the means to enforce reliable validation and authentication mechanisms without the need to replace surrounding infrastructure in the advent of a CRQC.[39] OT owners and operators should request crypto-agile features in ICS equipment acquisitions since reliable asymmetric encryption is vital for validating uncorrupted information and intended delivery channels.

OT or OT-connected devices at the network perimeter, especially those communicating over-the-internet, are likely to be priority candidates for post-quantum mitigation. These devices may serve as vectors for unauthorized remote access, corrupted instructions, or other messages to subordinate OT technology at long distances or in unsafe or difficult-to-access locations. Relevant best practices for establishing OT crypto-agility include:

- Configuring OT networks such that perimeter devices are ready to update or patch with little notice.[40,41]
- Maintaining vendor technology that complies with post-quantum standards, implementations, and frameworks.[42,43]
- Deploying platforms with crypto-agile encryption management mechanisms.[44,45]
- Applying Secure by Design and Secure by Default principles and sound cryptographic implementation.[46,47]

Update to Post-Quantum Algorithms

To the extent possible, critical infrastructure owners and operators should implement the latest post-quantum encryption standards.[ii] NIST released the first 3 finalized Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography on August 13, 2024. Some of these standards are designed for different aspects of encryption (e.g., key encapsulation mechanisms vs. digital signatures), so entities may need to adopt more than one.

Cryptographic mechanisms create processing demand for the systems that encrypt, decrypt, sign, and validate communications. Additional processing overhead from adding encryption mechanisms or upgrading existing ones may exceed current hardware capabilities in OT systems. Especially susceptible to performance constraints are systems considered to be legacy platforms or those manufactured before cryptographic standards became common.[48] In instances where platforms must migrate to post-quantum algorithms, OT owners and operators may be forced to replace some hardware or implement surrounding, capable architecture if core systems are not computationally sufficient to support post-quantum protections.

Other challenges with implementing or updating cryptographic mechanisms may affect OT system-level interoperability on a protocol or application basis. Original equipment manufacturing relationships with vendors and owner and operator dependencies on external service providers compound these interoperability concerns which may impact operational uptime, visibility, or compliance.[49,50] In relevant cases, manufacturers, vendors, and service providers share responsibility with OT owners and operators in maintaining safety and continuity as new cryptographic measures are implemented.

As quantum computing capabilities evolve, other post-quantum cryptographic standards may emerge. Critical infrastructure owners and operators should, on a prioritized basis, update systems to incorporate current and future standards.

Disclaimer

The information in this report is provided "as is" for informational purposes only. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring.

[ii] Some research suggests that implementing post-quantum algorithms may increase susceptibility to denial of service (DoS) or distributed denial of service (DDoS) resource exhaustion remote cyberattacks. See: https://eprint.iacr.org/2023/266.pdf.

[23] Government Accountability Office, Report to Congressional Requesters, "Information Technology: Federal Agencies Need to Address Aging Legacy Systems," GAO-16-468, May 2016, https://www.gao.gov/assets/gao-16-468.pdf. Accessed on September 26, 2024.
[24] Nuclear Regulatory Commission, "Instrumentation and Control System Failures in Nuclear Power Plants," https://www.nrc.gov/docs/ML0037/ML003757315.pdf. Accessed on September 26, 2024.
[25] Cybersecurity and Infrastructure Security Agency, Alert, "Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats," Last Revised July 5, 2022, https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats. Accessed on September 26, 2024.
[26] National Institute of Standards and Technology, "NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers," August 24, 2023, https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers. Accessed on September 26, 2024.
[27] National Institute of Standards and Technology, Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Accessed on September 26, 2024.
[28] Cybersecurity and Infrastructure Security Agency, "Layering Network Security Through Segmentation," January 2022, https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf. Accessed on September 26, 2024.
[29] National Institute of Standards and Technology, Special Publication 800-82, Revision 3, "Guide to Operational Technology (OT) Security," September 2023, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf. Accessed on September 26, 2024.
[30] David Garton, "Topic Paper 4-14: Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation," Plains All American Pipeline, Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure, November 12, 2019, https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Accessed on September 26, 2024.
[31] Cybersecurity and Infrastructure Security Agency, "Layering Network Security Through Segmentation," January 2022, https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf. Accessed on September 26, 2024.
[32] National Institute of Standards and Technology, Special Publication 800-82, Revision 3, "Guide to Operational Technology (OT) Security," September 2023, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf. Accessed on September 26, 2024.
[33] David Garton, "Topic Paper 4-14: Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation," Plains All American Pipeline, Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure, November 12, 2019, https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Accessed on September 26, 2024.
[34] Cybersecurity and Infrastructure Security Agency, "Layering Network Security Through Segmentation," January 2022, https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf. Accessed on September 26, 2024.
[35] National Institute of Standards and Technology, Special Publication 800-82, Revision 3, "Guide to Operational Technology (OT) Security," September 2023, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf. Accessed on September 26, 2024.
[36] David Garton, "Topic Paper 4-14: Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation," Plains All American Pipeline, Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure, November 12, 2019, https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf. Accessed on September 26, 2024.
[37] National Institute of Standards and Technology, Special Publication 800-63B, "B.4 Authenticators and Verifiers," https://pages.nist.gov/800-63-3-Implementation-Resources/63B/Authenticators/. Accessed on September 26, 2024.
[38] National Security Agency, Cybersecurity and Infrastructure Security Agency, Communications Sector Coordinating Council, Defense Industrial Base Sector Coordinating Council, Information Technology Sector Coordinating Council, "Developer and Vendor Challenges: Identity and Access Management," https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF. Accessed on September 26, 2024.
[39] Department of Homeland Security, "Cryptographic Agility," Infographic, May 12, 2022, https://www.dhs.gov/sites/default/files/2022-05/22_0512_plcy_2966-01_cryptographic-agility-infographic.pdf. Accessed on September 26, 2024.
[40] Cybersecurity and Infrastructure Security Agency, National Security Agency, National Institute of Standards and Technology, "Quantum-Readiness: Migration to Post-Quantum Cryptography," As of August 17, 2023, https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf. Accessed on September 26, 2024.
[41] Department of Homeland Security, "Cryptographic Agility," Infographic, May 12, 2022, https://www.dhs.gov/sites/default/files/2022-05/22_0512_plcy_2966-01_cryptographic-agility-infographic.pdf. Accessed on September 26, 2024.
[42] Cybersecurity and Infrastructure Security Agency, National Security Agency, National Institute of Standards and Technology, "Quantum-Readiness: Migration to Post-Quantum Cryptography," As of August 17, 2023, https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf. Accessed on September 26, 2024.
[43] Department of Homeland Security, "Cryptographic Agility," Infographic, May 12, 2022, https://www.dhs.gov/sites/default/files/2022-05/22_0512_plcy_2966-01_cryptographic-agility-infographic.pdf. Accessed on September 26, 2024.
[44] Ibid.

[45] National Institute of Standards and Technology, Cybersecurity White Paper, "Getting Ready for Post Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," April 28, 2021, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf. Accessed on September 26, 2024.
[46] Cybersecurity and Infrastructure Security Agency, "Secure by Design," https://www.cisa.gov/securebydesign. Accessed on September 26, 2024.
[47] National Institute of Standards and Technology, Computer Security Resource Center, "Cryptographic Standards and Guidelines," Updated October 24, 2023, https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines. Accessed on September 26, 2024.
[48] Department of Homeland Security, "Department of Homeland Security: Control Systems Communications Encryption Primer," December 2009, https://www.cisa.gov/sites/default/files/documents/Encryption_Primer_20091211_S508C.pdf. Accessed on September 26, 2024.
[49] Department of Homeland Security, "Recommended Practice for Patch Management of Control Systems," December 2008, https://www.cisa.gov/sites/default/files/2023-01/RP_Patch_Management_S508C.pdf. Accessed on September 26, 2024.
[50] Cybersecurity and Infrastructure Security Agency, "JCDC Remote Monitoring and Management Cyber Defense Plan," August 2023, https://www.cisa.gov/sites/default/files/2023-08/JCDC_RMM_Cyber_Defense_Plan_TLP_CLEAR_508c_1.pdf. Accessed on September 26, 2024.