Strategy for Migrating to Automated Post-Quantum Cryptography Discovery and Inventory Tools

Publication: August 15, 2024
Cybersecurity and Infrastructure Security Agency

Table of Contents

1. OVERVIEW

The mission of the Cybersecurity and Infrastructure Security Agency (CISA) is to lead the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure upon which Americans rely on every hour of every day. CISA serves as the operational lead for cybersecurity across the Federal Civilian Executive Branch (FCEB) and national coordinator for critical infrastructure security and resilience. To accomplish its mission, CISA connects stakeholders in industry and government to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience. Through direct services, guidelines, recommendations, directives, standards, and more, CISA and its partners work to promote a secure and resilient infrastructure for the American people.

On November 18, 2022, the Director of the Office of Management and Budget (OMB) issued Memorandum 23-02 (M-23-02), "Migrating to Post-Quantum Cryptography," to the heads of executive departments and agencies. M-23-02 includes instructions for reporting information about cryptographic systems that use quantum-vulnerable cryptography to the Office of the National Cyber Director (ONCD) and CISA. The instructions in M-23-02 include a task for CISA to develop a strategy on automated tooling and support for the assessment of agency progress towards adoption of post-quantum cryptography (PQC) in consultation with the National Institute of Standards and Technology (NIST) and the National Security Agency. This document contains the strategy developed by CISA.

Purpose

The purpose of this strategy is to support the assessment of FCEB progress towards PQC adoption using automated cryptography discovery and inventory (ACDI) tools.

Background

As outlined in National Security Memorandum (memo) 10, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," the threat posed by the prospect of a cryptanalytically-relevant quantum computer (CRQC) requires that agencies prepare now to implement PQC. Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure federal data and information systems.

Scope

This strategy applies to all FCEB systems, excluding national security systems (NSS),[1] operated by, or on behalf of, any agency. M-23-02 established requirements for agencies to inventory their active cryptographic systems. The first systems to be reported include any of the following:

1. A high impact information system;
2. Agency High Value Asset (HVA); or
3. Any other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks. Other systems should include information systems or assets that: contain data expected to remain mission-sensitive in 2035[2] or, are logical access control systems based in asymmetric encryption (such as Public Key Infrastructure) that use any of the algorithms listed in Appendix B of the memo.

1. For the purposes of this memorandum, "NSS" refers both to any information system described in 44 United States Code (U.S.C.) 3552(b)(6), "National Security System," as well as any system described in 44 U.S.C. 3553(e), "Department of Defense and Intelligence Community Systems".
2. This criterion refers to data that if recorded now, and later decrypted by a CRQC in 2035, would still be considered mission sensitive.

As used in M-23-02, the term "cryptographic system" means an active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: (1) creation and exchange of encryption keys; (2) encrypted connections; or (3) creation and validation of digital signatures.

This strategy includes discovery options for both cloud-based and on-premises information systems or assets. It also addresses deploying ACDI tools across the FCEB, using CyberScope for reporting Federal Information Security Modernization Act of 2014 (FISMA) metrics related to PQC adoption, and integrating the ACDI tools with the Continuous Diagnostics and Mitigation (CDM) Program.

Goals

The primary goal of this strategy is to enable the assessment of agency PQC transition progress. Included is the use of ACDI tools to support a FCEB agency in its creation of an inventory of its information systems and assets that contain CRQC-vulnerable cryptography. This strategy also supports an agency's annual submission of its inventory to ONCD and CISA. The inventory tools automate the collection of the cryptographic characteristics required for the inventory.

Another goal is to integrate ACDI tools with CISA's CDM Program, which may help to reduce the resources required to generate the inventory content.

On-Going Research Areas

There are three areas of on-going research and development that will inform and support PQC migration efforts:

1. The tools that detect and inventory the types of cryptography in use on assets are in various stages of development across industry.
2. CISA has not been able to confirm the full scope of cryptographic algorithm detection capabilities that will be available via automated cryptographic discovery tools. For example, it is not clear if these tools will be able to detect the embedded algorithms used within software packages, such as custom or government developed software.
3. CISA is a collaborator along with over 28 industry partners in the NIST National Cybersecurity Center of Excellence's (NCCoE) "Migration to PQC" project. The project's initial work with discovery and inventory tools will be leveraged to inform future versions of this strategy. For example, the NCCoE will soon publish guidance and information on discovery and inventory tools provided by its collaborators. This initial public draft will be NIST Special Publication (SP) 1800-38, "Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography," Volume B and will be posted for a public comment period to solicit input about how to make its guidance clearer to readers. CISA will incorporate aspects of that publication and look for ways to leverage additional activities in the NCCoE collaboration to inform the FCEB.

2. APPROACH

Inventory Data Items for Reporting

Section II of the M-23-02 memo requests nine data items for each reported cryptographic system. Most of the nine data items cannot be detected or collected using currently available automated tools, and therefore, are manually collected. However, three of the nine data items may be collected using ACDI or CDM[3]. These three

3. Note that CDM does not presently collect item 4 as part of the Software Asset Management (SWAM) capability.

data items from Section II of M-23-02 are as follows:

- Item 4 - For CRQC-vulnerable cryptographic system inventory elements (report):
  - Algorithm;
  - Service provided (an active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: (a) creation and exchange of encryption keys; (b) encrypted connections; or (c) creation and validation of digital signatures; and
  - Length of associated cryptographic keys.
- Item 5 - If the cryptographic system(s) is/are part of a software package, indicate whether the software package is:
  - Commercial-Off-the-Shelf and name of the vendor;
  - Government-Off-the-Shelf and name of the agency; or
  - Other (e.g., custom software) and name of the vendor/developer.
- Item 6 - Operating system(s), including major and minor version information, if applicable.

For item 4, all the information (e.g., metadata) required to identify CRQC-vulnerable software packages, file systems, database systems, or documents may not be available or discoverable using automated data. Digital certificates are an example where the information explicitly includes the desired data items.

Data Collection for Reporting

Once the PQC standards are finalized, it is expected that vendors will advertise their product plans or roadmaps, which may simplify the cryptographic system inventory process. For example, if vendors identify the product model or version that will be upgraded to PQC-hybrid mode or PQC-only mode operation, the cryptographic system inventory elements would be determined by discovering the model or version information for that product. This approach could apply to both internal and cloud assets.

Data Collection via ACDI Tools

ACDI tools, either individually or in combination, provide the following cryptographic discovery types: network, file system, database system, or software package – the combination of which enables discovery of encryption for data-in-transit and data-at-rest. The outputs of these tools may provide the needed information to generate data items listed in M-23-02 for cryptographic systems (see "Inventory Data Items for Reporting" above). The NIST NCCoE Migration to PQC Project's discovery and inventory demonstrations include a focus on common output elements that the tools could support.

Data Collection via CDM

The existing CDM capabilities may be able to provide the information needed to generate data item 5 (cryptographic system/software package) and data item 6 (operating system(s)) listed above. The extant SWAM capability within CDM[4] may be able to provide a partial or complete set of the requested information. With the integration of ACDI tools into CDM, cryptographic system characteristics should be available, as well as additional cryptographic information provided by ACDI tools.

4. Note that the information provided by SWAM capability within CDM presently has varying levels of fidelity due to lack of standardization and differences in vendor reporting.

Data Collection via Manual Means

At this time, there are no known automated tools that can collect the inventory information for the following items in Section II of M-23-02:

- **Item 1** – FISMA system identifier
- **Item 2** – The Federal Information Processing Standard 199 system categorization (Low, Moderate, or High)
- **Item 3** – If an HVA, the HVA identifier
- **Item 7** – Whether the information system or hosting information system(s) is/are hosted by:
    - The agency (on premise);
    - A commercially operated cloud service provider, in which case the name of the commercial provider must be supplied;
    - A government-operated cloud service provider, in which case the name of the agency provider must be supplied; or
    - A hybrid environment, in which case the name of the cloud service provider(s) must be supplied.
- **Item 8** – Lifecycle characteristics of the data contained in the system, including types of data (as described by national records management categories) and how long the data and associated metadata need protection (i.e., "time to live")
- **Item 9** – Any additional notes deemed relevant by the agency.

Additionally, software packages with embedded cryptography, customized applications, or certain operating systems may not be discoverable using automated tools. Agencies may have to identify and request vendors provide information describing the cryptography algorithms and key lengths for these software packages. Manual tracking of these products may need to be maintained.

Reporting

Figure 1 below depicts an overview of the data discovery, collection, and reporting approaches discussed throughout this document, i.e., cryptographic asset data via ACDI tools integrated with CDM, manual collection for assets not discovered by CDM or ACDI tools, and CyberScope reporting of FISMA metrics.

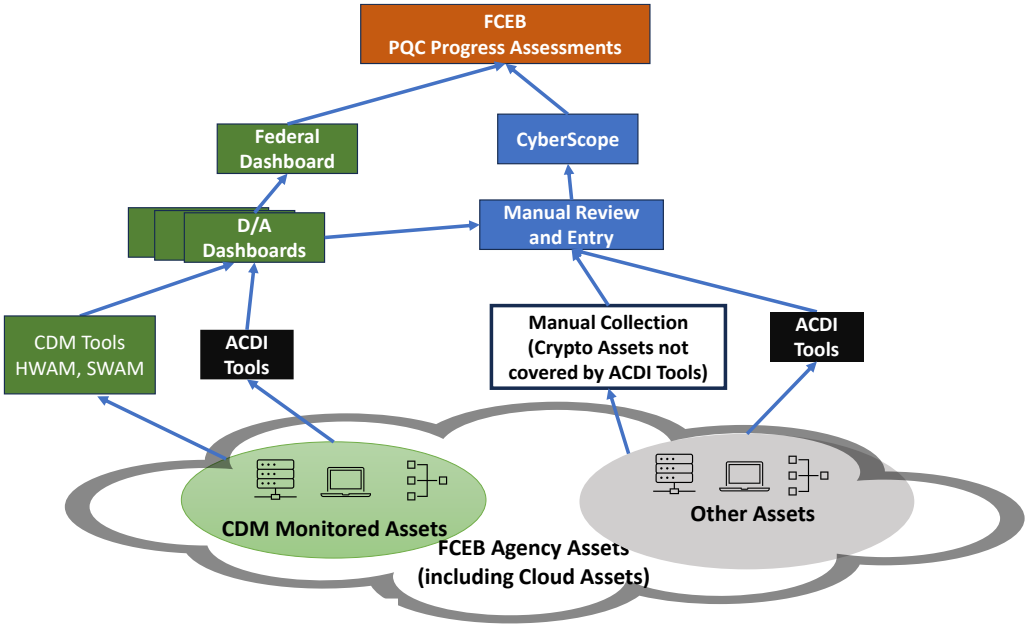

Figure 1 – Cryptographic Data Discovery, Collection, and Reporting

CyberScope

CyberScope is a spreadsheet form and the current inventory reporting mechanism that is submitted to CISA and ONCD. OMB's memo indicates that there will be future updates to FISMA requirements to support capturing the cryptographic system inventory. When the FISMA requirements are updated, CyberScope will also need to be updated to support those new requirements. After those requirements are incorporated into CyberScope, agencies will continue to report inventories via CyberScope.

CDM

The following components of the CDM capabilities will need to be enhanced to enable reporting of cryptographic system inventory discovered by ACDI tools:

- **CDM logical data model** – expanded to include data elements needed to store cryptographic inventory characteristics.
- **CDM asset management sensors** – expanded to include ACDI tools. The specific set of tools cannot be determined until the tool vendors announce their product capabilities, and tool testing verifies capabilities.
- **CDM agency and federal dashboards' content** – interfaces, displays, and analytics will need expanding to support data elements provided by ACDI tools.

ACDI Tool Development and Integration

The following high-level steps are necessary to develop and integrate ACDI tools:

1. When suitable ACDI tools are available, execute a pilot program to integrate ACDI tools into the CDM tool suite. This pilot would determine the optimal level of integration including data elements and interfaces. For assets discovered by CDM, integration would reduce the level of effort required to create cryptographic inventories, needed to report to ONCD and CISA for PQC adoption tracking. As part of this pilot program, a comparative analysis should be conducted to determine the extent that ACDI tools can

discover cryptographic assets vice those assets known via manual means.

2. CDM updates should consider modifications to the dashboards, logical data model and data dictionary to include new PQC transition related metrics. Dashboard updates may include computed information from data collected by CDM and ACDI tools. For example, the specific software package utilizing a CRQC-vulnerable cryptographic algorithm may require a look-up function to correlate the results of an ACDI tool with SWAM data.
3. Additionally, once ACDI tools are available, such tools should be added to the CDM approved products list. This will require updates to the CDM Program Technical Capabilities Volume Two: Requirements Catalogue to account for ACDI capabilities and required features.
4. Enhance CyberScope to support FISMA PQC transition metrics. CISA understands that OMB will be enhancing FISMA requirements to enable assessments of the transition to full PQC adoption.
5. Maintain situational awareness of the industry trends to identify opportunities to reduce the resources needed to assess the FCEB agencies progression towards PQC adoption. Procurement processes should include requirements for secure by design principles that provide assurance that PQC cryptography is included in future products as soon as feasible and implemented securely. Also, as they become familiar with industry offerings, agencies should share information with other agencies about which products and version numbers are PQC compliant.
6. For assets not discovered by CDM, agencies will continue to manually report inventory to ONCD and CISA via the current spreadsheet form. Agencies will report via CyberScope when updated with new FISMA reporting requirements.

The following notional timeline provides a high-level schedule of activities necessary to achieve the strategy described.

	Milestone / Activity	Agency	CY 2023	CY 2024	CY 2025	CY 2026	CY 2027	CY 2028	…	CY 2035
PQC Reporting	PQC Reporting Strategy Released	CISA/NSA/NIST	✓							
	PQC Reporting Strategy Annual updates (as needed)	CISA/NSA/NIST								
	All FCEB agencies reporting (includes May 2023 report)	FCEB	✓							
PQC Reporting Tools Capability	Complete status assessment of ACDI tools	NIST	✓							
	Pilot the integration of ACDI tools with CDM	CISA								
	Deploy ACDI tools into CDM	CISA								
	Enhance Cyberscope for PQC reporting via FISMA metrics	CISA								
	Release/update PQC compliant products list	CISA								
	Deploy ACDI tools for non-CDM assets	FCEB								

Identification and Remediation of PQC Migration

Once the described enhancements and updates are made, CDM dashboards and CyberScope reports can be compared to the list of PQC-compliant products noted in item 4 of the "ACDI Tool Development and Integration" section above. Through comparing these lists, CISA can identify systems, or agencies struggling to implement the products necessary for the PQC transition. CISA will offer support to accelerate their PQC adoption efforts or identify products with complex or vulnerable cryptographic implementations for mitigation actions.

3. REQUIRED ACTIONS

a. Within 30 days of release of this memo, CISA will begin to monitor and maintain the status of Migration to PQC throughout what is known will be a long transition period. CISA will continue to monitor FCEB reporting on the use of quantum-vulnerable cryptography and support FCEB remediations of quantum-vulnerable cryptography as part of its overall monitoring portfolio.

b. Within 90 days of receipt of PQC transition FISMA metrics from OMB, CISA will update CyberScope to support these reporting requirements.

c. Within 360 days of successful completion of the pilot program, CISA will update the CDM program to support integrated ACDI tools as noted in item 2 of the "ACDI Tool Development and Integration" section above.

d. Within 90 days of release of this memo, CISA will work with the General Services Administration to develop and maintain a list of PQC enabled products (with version numbers) for cryptographic systems.

e. Within 30 days of release of this memo, NIST will publish its initial draft of NIST SP 1800-38A documenting its demonstrations of discovery and inventory tools.

f. Within 30 days of NIST publishing the initial public draft of NIST SP 1800-38 Volume B, CISA will initiate a pilot program in accordance with item 1 of the "ACDI Tool Development and Integration" section above.

g. Results of this pilot program will be shared within 180 days of start.

h. Within 120 days of CISA updating CDM for the integration of ACDI tools, FCEB agencies will begin planning for deployment of updated CDM tools and dashboards.

i. Within 120 days of successful completion of the pilot program, FCEB agencies will begin planning for deployment of ACDI tools for assets not discovered by CDM.

APPENDIX A: ACRONYMS

Acronym	Expanded
ACDI	Automated Cryptography Discovery and Inventory
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CRQC	Cryptanalytically-Relevant Quantum Computer
FCEB	Federal Civilian Executive Branch
FISMA	Federal Information Security Modernization Act of 2014
HVA	High Value Asset
M-23-02	Memorandum 23-02
Memo	Memorandum
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NSS	National Security System
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
PQC	Post-Quantum Cryptography
SP	Special Publication
SWAM	Software Asset Management
U.S.C.	United States Code