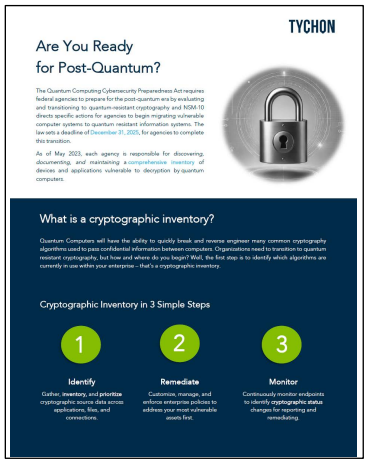
TYCHON

carahsoft.



Are You Ready for Post-Quantum?

Thank you for downloading this TYCHON resource! Carahsoft is the public sector distributor for TYCHON solutions.

To learn how to take the next step toward acquiring TYCHON's solutions, please check out the following resources and information:

For additional resources:
carah.io/TYCHONResources

For upcoming events:
carah.io/TYCHONEvents

For additional TYCHON solutions:
carah.io/TYCHONProducts

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
TYCHON@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/TYCHONContracts

For more information, contact Carahsoft or our reseller partners:
TYCHON@carahsoft.com | 844-445-5688

TYCHON

Are You Ready for Post-Quantum?

The Quantum Computing Cybersecurity Preparedness Act requires federal agencies to prepare for the post-quantum era by evaluating and transitioning to quantum-resistant cryptography and NSM-10 directs specific actions for agencies to begin migrating vulnerable computer systems to quantum resistant information systems. The law sets a deadline of December 31, 2025, for agencies to complete this transition.

As of May 2023, each agency is responsible for *discovering, documenting, and maintaining* a comprehensive inventory of devices and applications vulnerable to decryption by quantum computers.

What is a cryptographic inventory?

Quantum Computers will have the ability to quickly break and reverse engineer many common cryptography algorithms used to pass confidential information between computers. Organizations need to transition to quantum resistant cryptography, but how and where do you begin? Well, the first step is to identify which algorithms are currently in use within your enterprise – that's a cryptographic inventory.

Cryptographic Inventory in 3 Simple Steps

1

Identify

Gather, **inventory,** and **prioritize** cryptographic source data across applications, files, and connections.

2

Remediate

Customize, manage, and enforce enterprise policies to address your most vulnerable assets first.

3

Monitor

Continuously monitor endpoints to identify **cryptographic status** changes for reporting and remediating.

How To Generate a Cryptographic Inventory with ACDI

Automated Cryptography Discovery & Inventory (ACDI) tools are systems designed specifically to help agencies meet the requirements of the Quantum Computing Cybersecurity Preparedness Act. TYCHON Quantum Readiness is an ACDI that delivers a comprehensive and prioritized inventory of cryptographic systems using the Identify, Remediate, Monitor three-part approach.

1

Identify Current Cryptography

TYCHON uses precompiled dashboards, aligned to both Splunk and Elastic platforms, to search your enterprise data across applications, files, and connections and report:

- All algorithms in use, service provided, and length of keys
- Risk-scored cryptographic inventory for executables and databases (in-transit and at-rest)
- List of vulnerable systems and devices across most modern and legacy Windows and Linux OSs.

TYCHON Quantum Readiness meets and exceeds NIST discovery, inventory, and architecture requirements. TYCHON automatically discovers, maps, and assesses NIST 1800-38B criteria and satisfies NIST Test Case Scenarios. This includes capturing Public Key, TLS, Client and Server Certificates, Key Encapsulation Methods, Signatures, Symmetric Ciphers and MAC algorithms, listening ports, executables (even those not running on the network) and more. In addition, TYCHON's flexible architecture and design aligns to NIST 1800-38C.

Once you gather the data, the next challenge is to make sense of the cryptographic inventory. This is why TYCHON simplifies the visual representations using clear dashboards with built-in cryptographic risk categories. TYCHON dashboards group Cryptographic Risk into 5 categories from Level 1, most secure and NIST approved, down to Level 5, which should never be used under any circumstances. The list is continuously updated to reflect new risks and NIST / NSA protocols as they arise.

*Use built-in cryptographic **risk categories** to assess and prioritize.*

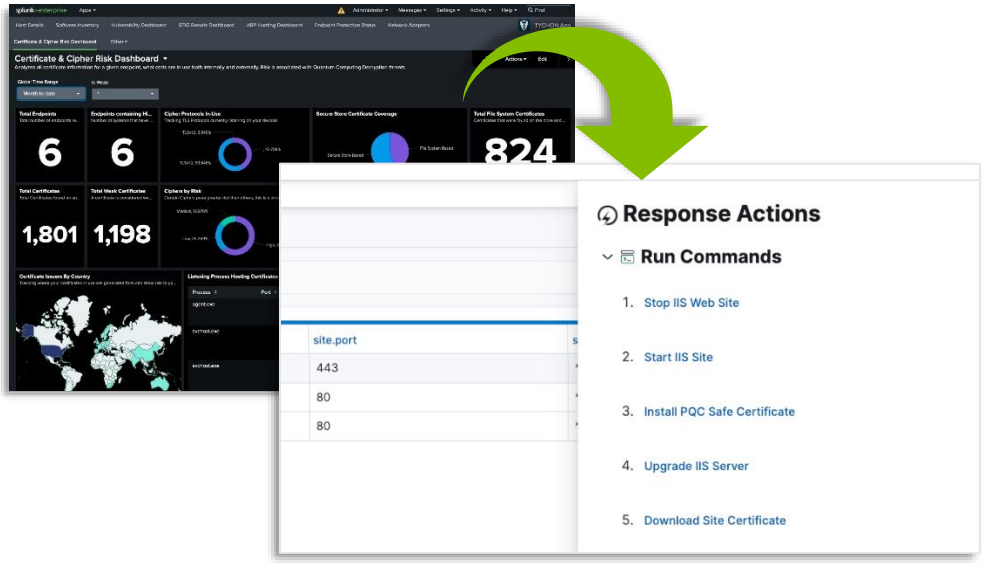
TYCHON

AYR_202502_002 | February 2025

2

Remediate On Demand

TYCHON Quantum Readiness identifies cryptographic risks using clear and simple dashboards. Then, using the same ACDI tool, users can immediately remediate identified risks via our Response Action feature. This easy-to-use option lets users target endpoints directly from the dashboards and respond with actions such as disabling weak ciphers, quarantining at risk systems, removing software, and more.



3

Monitor Cryptographic Status Changes

TYCHON provides the ability to set up custom alerts based on risk categories or cryptographic inventory changes. This enables you to continuously monitor endpoints to identify risk and ensure comprehensive visibility.

One of the challenges for managing cryptographic inventory is the constant state of change. This is why TYCHON Quantum Readiness was built with Crypto-agility in mind. As new risks and NIST/NSA protocols arise, the TYCHON dashboards and associated risk scores can be easily updated to reflect these changes.

About Tychon

Learn More: tychon.io

Tychon LLC is a software company founded by former U.S. Department of Defense cybersecurity experts. TYCHON, our core product, is the world's first advanced endpoint analytics and remediation platform designed to be the "gold source" for enterprise endpoint data. It provides the ability to search, visualize, remediate, and monitor security concerns across all endpoints within one powerful interface. TYCHON delivers a flexible endpoint management query and response tool that gives administrators and incident responders complete control of their systems.