SCOPING PAPER: *NATIONAL PREPAREDNESS FOR POST-QUANTUM CRYPTOGRAPHY*

INTRODUCTION

Established in 1982, the President's National Security Telecommunications Advisory Committee (NSTAC) is an industry advisory body that provides the president with advice on the information and communications technology ecosystem with respect to national security, cybersecurity, and emergency preparedness concerns. In May 2024, the administration and NSTAC discussed a potential new study, "*National Preparedness for Post-Quantum Cryptography (PQC),*" which has not yet been tasked officially.

BACKGROUND AND PROPOSED SCOPE OF STUDY

The National Cybersecurity Strategy includes a strategic objective to prepare for a post-quantum future, urging the private sector to follow the model of the U.S. government (USG) as it prioritizes the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments and develops complementary mitigation strategies to provide cryptographic agility in the face of known and unknown future risks and threats.

As described in National Security Memorandum 10 (NSM-10), *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, when cryptanalytically relevant quantum computers are available, they could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions. As NSM-10 noted, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as feasible by 2035. Last year, the National Institute of Standards and Technology (NIST) selected four algorithms designed to withstand attacks by quantum computers. NIST plans to finalize standards for use of these algorithms by the end of 2024.

Driving ecosystem-wide adoption of emerging PQC standards or even adoption by a critical mass of public and private sector organizations that support critical infrastructure and protect the United States' sensitive data, including stored data, will be a complex endeavor. It will require coordination across service providers and silicon solution companies, and original equipment manufacturers will need to integrate those solutions. Additionally, it will require broader efforts in standards and open-source communities to support integration into key protocols as well as creation of production-grade open-source code, libraries, and co-pilots. Adopting these technologies may require expensive updates to hardware and software cryptography. In addition, relevant stakeholders must be made aware of these standards and the imperative to migrate toward their adoption.

To support the nation's preparedness for its post-quantum future, the NSTAC will identify barriers to critical infrastructure providers adoption of PQC standards and provide recommendations on how to reduce these barriers in anticipation of the advent of quantum computing over the next decade. To inform these recommendations, the study will consider lessons learned in past technological transitions and include conversations with critical infrastructure providers, USG agencies, and non-federal public

institutions to understand what support they need to adopt PQC standards when that technology becomes available.

KEY FOCUS AREAS TO CONSIDER

Implementation of Current Cryptography Standards:

- What are the current cryptography standards being used today?
- What is the average level of adoption for the current standards?
- What process is followed for adoption / implementation of the current standards?
- What is the average time to implement the current standards?
- What are key components that are required for the adoption of these standards, from production grade code, libraries, and co-pilots to optimized hardware implementations?

Implementation of PQC:

- What is the status of PQC, including algorithms, reference implementations, production grade libraries, and supporting infrastructure?
- How do PQC algorithms perform for general ecosystem wide needs (e.g., TLS, DNSSec, x.509 certificates) compared to classical alternatives?
- What steps should be performed by entities to execute a smooth, timely, and repeatable process for PQC implementation, including testing, validation, deployment, and maintenance of the new cryptographic solutions?
    - What framework(s) or roadmap(s) exist that establish a standard and repeatable process to help guide organizations in PQC implementations (e.g., risk assessments, inventory solutions, tactical roadmaps, etc.)?
- What are the best practices and methods to ensure the interoperability and compatibility of PQC solutions with existing cryptographic infrastructure, legacy systems, and other internationally adopted PQC solutions?
    - To what extent are countries globally adopting similar or interoperable PQC standards?
- How should the USG think about monitoring and evaluating the effectiveness and impact of the PQC transition?
- How can the PQC-based technologies be architected to maintain crypto-agility and remain resilient during the time before PQC algorithms are fully validated and standardized?
- What additional requirements need to be addressed for hybrid implementations?

Barriers to Implementation of PQC

- What challenges (e.g., awareness, readiness, education and training, speed to implementation, etc.) might complicate the transition to PQC?
- What are the challenges and risks of managing the coexistence and transition between classical and quantum-resistant algorithms?
- What principles should guide how to manage and mitigate the risks and challenges associated with the PQC transition, such as protection of stored data, backward compatibility, cost and complexity, and human factors?

- What technology will have challenges in transitioning to PQC and will other approaches need to be taken to manage the risks?
    - How effective will PQC algorithms integrate with operational technology (OT) systems?
- What are cross sector dependencies and challenges in the adoption of PQC?
    - What are, some examples of, sector specific dependencies?
- What are the dependencies and challenges in designing for crypto agility, which may allow future upgrades to better (e.g., faster or more secure) PQC algorithms.

Additional Policy Opportunities:

- How can the USG support and incentivize critical infrastructure owners to transition to PQC?
- What opportunities exist for the USG to address any identified challenges (e.g., selection of PQC algorithm(s), speed of adoption, education and training, interoperability, etc.)?
- How can the USG help with international coordination and engagement?
- How should USG incentivize continuous investment in new cryptographic algorithms and standards, including those based on new mathematical problems?
- How should USG work with researchers on vulnerabilities in core mathematical assumptions around PQC algorithms?