Preparing for Post-Quantum Critical Infrastructure

Assessments of Quantum Computing Vulnerabilities of National Critical Functions

MICHAEL J. D. VERMEER, EDWARD PARKER, AJAY K. KOCHHAR

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

An FFRDC operated by the RAND Corporation under contract with DHS

This research was published in 2022.

About This Report

The Homeland Security Operational Analysis Center (HSOAC) is carrying out a project entitled "National Critical Function Emerging Risk Analysis" for the National Risk Management Center (NRMC) of the Cybersecurity and Infrastructure Security Agency (CISA). This project is intended to help CISA provide its leadership and critical infrastructure owners and operators greater awareness of emerging threats and hazards and recommendations on how to manage the risks resulting from these threats and hazards.

Under the auspices of this project, HSOAC was asked to perform an analysis of the vulnerabilities in national critical functions (NCFs) from future quantum computing capabilities. This report describes a high-level assessment of the quantum computing vulnerabilities affecting each of the 55 NCFs. Those assessments are intended to help CISA understand the issues affecting each NCF and prioritize U.S. government assistance to critical infrastructure owners and operators. The findings should be of interest to critical infrastructure owners and operators and the U.S. government agencies that support and partner with them to protect critical infrastructure.

This research was sponsored by the NRMC and conducted within the Strategy, Policy, and Operations Program of the HSOAC federally funded research and development center (FFRDC).

About the Homeland Security Operational Analysis Center

The Homeland Security Act of 2002 (Section 305 of Public Law 107-296, as codified at 6 U.S.C. § 185) authorizes the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology, to establish one or more FFRDCs to provide independent analysis of homeland security issues. The RAND Corporation operates HSOAC as an FFRDC for the U.S. Department of Homeland Security (DHS) under contract HSHQDC-16-D-00007.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. The HSOAC FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under task order 70RCSA21FR0000023, National Critical Function Emerging Issue Risk Analysis.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information on HSOAC, see www.rand.org/hsoac. For more information on this publication, see www.rand.org/t/RRA1367-6.

Acknowledgments

We would like to thank Andrew Lauland, Anu Narayanan, and Patricia Stapleton of the RAND Corporation for their leadership of the National Critical Function Emerging Issue Risk Analysis project. This effort would not have been possible without their support and guidance. We would also like to thank Christian Lowry of the NRMC and Nicholas Reese of DHS for their contributions. We also acknowledge Natalie Ernecoff, Shira H. Fischer, and Zachary Predmore of the RAND Corporation for their contributions. Finally, we would like to acknowledge the valuable contributions of the peer reviewers of this report, James Dimarogonas, Quentin E. Hodgson, and Daniel M. Gerstein of the RAND Corporation.

Summary

Quantum computers, devices that use properties of quantum mechanics to perform new computational operations, are expected to one day be capable of quickly solving the challenging mathematical problems underlying deployed public-key cryptography algorithms, thereby undermining a foundational building block of the global information security architecture. In anticipation of this event, the National Institute of Standards and Technology is executing a project to standardize new cryptographic algorithms, known as post-quantum cryptography (PQC), that will be resistant to the capabilities of quantum computers. However, the adoption of PQC across the United States is likely to be a long, challenging, and costly process. Historically, the adoption of new cryptographic standards and protocols has often taken decades to complete, and there is evidence to suggest that the transition to PQC could be much more challenging than many previous transitions (Vermeer and Peet, 2020). Moreover, although it is uncertain when a sufficiently capable quantum computer will be created, some risks might need to be addressed well before that event, and there might be little to no margin of time to delay adoption of PQC.

As part of its ongoing effort to support the security and resilience of critical infrastructure, the National Risk Management Center of the Cybersecurity and Infrastructure Security Agency tasked the Homeland Security Operational Analysis Center with assessing the quantum computing vulnerabilities affecting the national critical functions (NCFs) identified by the U.S. Department of Homeland Security (DHS). Although quantum computers might one day have many use cases that are relevant to the mission of DHS, the application of quantum computing to cryptographic problems is the primary use case that carries a well-defined risk. The intent of this task was to provide the Cybersecurity and Infrastructure Security Agency with the context needed to guide and prioritize efforts to engage the critical infrastructure community on this risk. We approached this task by creating individual, high-level assessments of each of the 55 NCFs. These assessments began with synopsizing the key issues and concerns related to quantum computing vulnerabilities for each NCF. Each synopsis describes how an NCF is affected by two categories of vulnerabilities: catch and exploit (the ability for an adversary to capture encrypted data in transit now and reveal it later when it possesses a quantum computer) and authentication (vulnerabilities associated with maintaining secure remote access to systems). The assessments rate each NCF in categories of urgency, scope, and cost per organization. Finally, the assessments consider other factors that will mitigate or exacerbate the vulnerabilities the NCF will experience, then combines all of these ratings into an assessment of priority for assistance.

Key Findings

All 55 NCF assessments are included in Appendix B, available online. Upon completion of the NCF assessments, we rated six of the NCFs as a high priority for assistance, 15 as medium priority for assistance, and 34 as low priority for assistance. Three NCFs were identified as critical enablers of the PQC migration:

- NCF 3, Provide Internet Based Content, Information, and Communication Services
- NCF 35, Provide Identity Management and Associated Trust Support Services
- NCF 52, Provide Information Technology Products and Services.

Stakeholders responsible for these NCFs will need to provide the key tools that allow the rest of the NCFs to migrate to PQC. Stakeholders in these critical enabling NCFs not rapidly producing the requisite products and services would broadly delay the overall migration to PQC across critical infrastructure and cause substantial vulnerability to persist into the future.

Another group of assessments had significant commonalities based on the NCFs' dependence upon integrated information technology and industrial control systems. Eighteen NCFs fell within this group. These assessments were defined largely by discussion of quantum vulnerabilities uniquely applicable to industrial control systems, although many of these assessments had other concerns unique to the given NCF. The generally low urgency for these NCFs and the growing use of defense-in-depth strategies in industry made most of these NCFs a low priority for assistance, although some NCFs with particularly challenging requirements for secure communication and control of operational technology might be higher priority for assistance.

Finally, we identified four key, cross-cutting findings upon completing the assessments:

- **All NCFs will need to prepare for the migration to PQC—even those that received low ratings in the assessments.** Every NCF stakeholder should take steps to improve cryptographic agility and prepare for the migration to PQC following the DHS roadmap.
- **Completely addressing quantum computing vulnerabilities will require robust adoption of PQC by most stakeholders across the NCFs, but much of the vulnerability can quickly be addressed if the migration is prioritized by relatively few entities.** That is, although change needs to happen very widely across many thousands of stakeholders across critical infrastructure, a lot of the vulnerability can be mitigated if a much, much smaller number of stakeholders make a few critical changes. Quantum computing vulnerabilities will be fully addressed only when enough stakeholders have migrated to the point at which prior vulnerable standards can be deprecated (a state in which an information system no longer allows the use of an out-of-date communication standard or protocol). However, a relatively small number of key changes by stakeholders in the critical enabling NCFs would likely mitigate a significant portion of the broader vulnerability and allow a robust start to the migration nationally.
- **Practical challenges in executing catch-and-exploit campaigns mean that very few NCFs likely need to urgently address catch-and-exploit vulnerabilities, although many NCFs will exhibit them.** Campaigns to capture sensitive data and hold them for later decryption are likely to be challenging and resource-intensive. Although many NCFs transmit data that will need to stay confidential for a long duration, only a few NCFs are likely to handle data that an adversary would consider valuable enough to invest resources in in such a long-term campaign.
- **Many factors related to the PQC migration are still unknown or uncertain. It is not yet clear what elements of the migration will present serious challenges for NCF stakeholders.** These assessments identify important context to inform engagements with stakeholders, but many important factors might be understood only through further detailed analysis in consultation with subject-matter experts and NCF stakeholders as they prepare for the PQC migration.

Contents

Tables

CHAPTER ONE

Introduction

Recent events have shown that critical infrastructure has significant cyber vulnerabilities, and attackers have frequently taken advantage of these vulnerabilities to devastating effect in and outside of the United States. Attacks have resulted in multiple high-profile disruptions to organizations providing national critical functions (NCFs), which are defined as "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (National Risk Management Center [NRMC], 2019, p. 1). The effects of cyberattacks include disruptions associated with NCFs, such as transport of materials by pipeline (Morrison, 2021), transport of cargo by vessel (Greenberg, 2018), production of chemicals (Voreacos, Chiglinsky, and Griffin, 2019), provision of medical care (Weiner, 2021), generation of electricity (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2021), and supply of water (Collier, 2021).

Although U.S. government agencies, as well as private organizations, have developed actions to prevent and respond to ongoing cyber-threats to critical infrastructure, another type of cybersecurity threat looms in the future due to the advances made possible through quantum computing. The security of the U.S. information and communication infrastructure is currently predicated on the assumption that it is impractically hard for computers to solve certain mathematical problems, such as integer factorization and finding the discrete logarithm of elliptic curves, and, therefore, sensitive communications can be adequately secured using cryptographic systems based on those problems. However, in 1994, Peter Shor showed that it would be possible for capable quantum computers to solve these mathematical problems much more rapidly than conventional computers can (Shor, 1994), opening up new vulnerabilities.

Quantum computing will not affect all types of cryptography equally and will have the most significant impact on current public-key cryptography systems, which use separate keys for encryption and decryption. These systems, which are currently ubiquitous in global infrastructure, provide the basis for a variety of mechanisms that facilitate secure, remote interactions over networks, including digital signatures, digital certificates used in public-key infrastructures (PKIs), and exchange of cryptographic keys used for communications (Vermeer and Peet, 2020). Fortunately, public-key cryptography algorithms have been an active area of research for decades. Some alternative public-key cryptography schemes depend on different mathematical problems that are expected to also be impractical for capable quantum computers to solve. Using these schemes should provide effective security even against capable quantum computers.

In response to the looming cybersecurity threat from quantum computing, the National Institute of Standards and Technology (NIST) began a process to create a new standard for public-key cryptography that is resistant to quantum computers. This new standard is known as *post-quantum cryptography* (PQC), and it will use known, alternative cryptographic algorithms that are impractical for both conventional and quantum computers to decrypt. NIST has been evaluating submitted post-quantum algorithms since 2017 and gathering regular feedback from the community. The organization recently announced the third round of candidate schema that it is evaluating for the standard and expects to have a draft standard available between 2022 and 2024 (Computer Security Resource Center, 2021b). Although undiscovered weaknesses in any of the

finalist algorithms might be discovered in coming years as they continue to undergo further cryptanalysis, the NIST process is likely to produce a robust standard. The classes of cryptography being considered have been subjects of research for many years, the finalist algorithms have been the subject of particularly focused cryptanalysis during the standardization process, and the final standard will include multiple algorithms that will provide redundancy should one or more of them be found wanting. Once the standard is released, it can begin to be incorporated into information systems across the United States (and, ideally, the world) to protect these systems against adversaries with quantum computers.

The adoption of PQC across the United States is likely to be a long, challenging, and costly process, however. Historically, the adoption of new cryptographic standards and protocols often takes decades to complete. Previous transitions to new standards for symmetric-key cryptography (e.g., the Advanced Encryption Standard), hash functions (e.g., secure hash algorithm 2), and secure Internet communication protocols (e.g., transport-layer security [TLS]) all took more than 15 years to achieve nearly complete adoption (Vermeer and Peet, 2020). There is also evidence to suggest that the transition to PQC could be much more challenging than many previous transitions. The transition will be much more extensive than some previous transitions (e.g., incorporating it into updates to multiple communication protocols, rather than moving to a new version of a single protocol) and involve more-significant changes that will cause compatibility challenges (e.g., larger key sizes) (Vermeer and Peet, 2020). Moreover, some risks must be addressed well before a cryptographically relevant quantum computer (CRQC) even exists,[1] and there might be little to no margin of time to delay adoption of PQC.

NIST recently published a document on the migration to PQC that is intended to complement the standardization process (Barker, Souppaya, and Newhouse, 2021). It describes ongoing NIST efforts to facilitate the migration, considerations for migration, and details of several demonstration migration scenarios. NIST's efforts include plans to discover

- all instances in which NIST Federal Information Processing Standards special publications and other guidance documents need to be updated
- standards that need updates or replacements from standard-development groups, such as the International Organization for Standardization and the Institute of Electrical and Electronics Engineers, and industry groups, such as the Trusted Computing Group (TCG)
- networking protocol standards, such as those from the Internet Engineering Task Force, that need to be updated or replaced.

In addition, the National Cybersecurity Center of Excellence has formed an applied-cryptography community of interest, in partnership with NIST and the Cybersecurity and Infrastructure Security Agency (CISA), to facilitate preparation for migration. NIST recently posted a white paper entitled "Getting Ready for Post-Quantum Cryptography" to inform discussion among this community (Barker, Polk, and Souppaya, 2021).

Finally, the U.S. Department of Homeland Security (DHS) also recently posted information detailing its approach to the PQC migration (DHS, 2021). The webpage describes a plan for DHS and its components to

[1] Quantum computers exist today, but they do not yet possess capabilities advanced enough to practically affect the cryptographic systems currently in use. Expert consensus is that a quantum computer capable of breaking encryption currently in wide use will not be available until approximately 2030 at the earliest (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing, 2019). Throughout this report, we use the term *CRQC* to describe a future quantum computer that would have such capability. Every mention of a quantum computer in this report should be assumed to refer to a CRQC.

make the migration to PQC, collaboration with NIST on tools to manage the transition, and a roadmap of steps stakeholders can take now to begin preparing for the migration.

Focus of This Study

To prepare for the eventual adoption of PQC, the NRMC asked the Homeland Security Operational Analysis Center (HSOAC), a federally funded research and development (R&D) center operated by the RAND Corporation, to assess the quantum computing vulnerabilities affecting NCFs. This assessment focused specifically on issues associated with implementations of cryptography that are robust against conventional computers but that will be vulnerable to a sufficiently capable quantum computer. This effort is part of HSOAC's broader project for CISA on analyzing emerging risks to the NCFs.

HSOAC's objective is to help CISA prioritize NCFs that might benefit most from U.S. government engagement and assistance. In support of this objective, we performed a high-level analysis of the entire set of 55 NCFs identified by DHS. This analysis includes assessments of multiple factors related to quantum computing vulnerabilities and challenges in migrating to PQC. The outcome of the effort is a categorization of NCFs according to priority for assistance, accompanied by the context needed to justify that categorization and inform initial engagements with representatives from the NCFs.

Scope of This Assessment

Quantum computing might eventually enable other use cases with security implications (e.g., applications to artificial intelligence), but, currently, cryptographic applications of quantum computing are the only known use case that presents a well-defined risk of concern to CISA. The risk arises from specific cybersecurity vulnerabilities that will be enabled by sufficiently capable quantum computers. The need to comprehensively identify the presence of those specific cybersecurity vulnerabilities across the whole set of NCFs presents a significant challenge. Information technology (IT) facilitating secure communications and remote management is ubiquitous across U.S. infrastructure, and the comprehensive identification and inventory of it was not feasible within the scope of this project. Therefore, with CISA's agreement, we simplified the scope of the analysis by taking an approach that focused at a high level on two questions for each NCF:

- What categories of systems that use vulnerable cryptography are used by the NCF?
- Could the exploitation of those vulnerabilities by an adversary with a quantum computer lead to a degradation or disruption of the function?

The focus on these questions allowed us to narrow the scope of the analysis in a few important ways:

- First, the assessments are focused solely on categories of systems that are remotely accessible and use cryptography vulnerable to quantum computing. In the analysis, we did not address other conventional cybersecurity issues (e.g., software security flaws, unsecured systems, or use of weak passwords), instead focusing exclusively on the use of a capable quantum computer to perform decryption operations on cryptography that is otherwise robust against decryption by conventional computers. Other cryptographic systems, such as symmetric-key cryptography and hashing, are not vulnerable to the same degree as public-key cryptography and are also generally not addressed. Exceptions to this latter case arise when systems currently use relatively weak symmetric keys that would not be practical to derive with a conventional computer but could present a vulnerability to an adversary with a quantum computer.

- Second, the assessments exclude a more general examination of the variety of negative outcomes that could affect an NCF, opting instead for a focus on a singular end outcome: *whether exploited vulnerabilities could significantly degrade or disrupt the function*. This focus was chosen because of the challenge presented by the differing scale and scope among the NCFs as they are currently defined. Some exploited vulnerabilities might be devastating to individual organizations that support an NCF, but, if an NCF is likely to be resilient to the failure of that organization (or other impacts), then even a very likely outcome that would be catastrophic to that organization might not factor heavily in the overall assessment for the NCF. If, however, there are likely to be cascading impacts on the function from a single failure, the potential for broad loss of trust in systems from a single high-profile incident, or vulnerabilities that are shared across many organizations (e.g., a vulnerability in a communication protocol used by every major organization in the NCF), then that vulnerability would factor heavily in the assessment. Consider the example of intellectual property (IP) theft in the discussion of NCF 49, Produce Chemicals. A single organization failing to address a vulnerability that leads to stolen IP might have little impact on the NCF as a whole. If, however, every organization that falls under the NCF shares this vulnerability, leading to *widespread* IP theft, then this vulnerability could lead to a degradation or disruption of the function over time—a notable impact to consider in the assessment for that NCF. Impacts that occur at a lower level of abstraction than *degradation or disruption of an NCF* are considered and occasionally described in the assessments, but their effects are considered in the analysis only inasmuch as they do or do not contribute to that key metric. To a significant degree, this metric depends on assessments of the well-known security triad of confidentiality, integrity, and availability.[2] Other specific context on the use and application of this metric is described in Appendix A, Methods Used in the Assessments.
- Finally, at the NRMC's request, much of the analysis also intentionally excludes detailed assessments of specific potential threat actors. In the analysis, we therefore assumed that any potential adversary would have access to a well-resourced CRQC but made few assumptions about an adversary's motivations. Essentially, in most cases, we asked the question, "What *could* an attacker do?" rather than "What would an attacker *want* to do?"

We intentionally performed this analysis at this high level to allow for a feasible landscape assessment of the set of NCFs and the priority for assistance. Many of the important details that are necessarily excluded from the scope described above could be addressed in follow-on assessments that take a detailed look at NCFs that this report identifies as high priority.

Overview of Our Approach

In this section, we provide a brief overview of the approach used to assess the NCFs, including definitions of key terms and distinctions between different types of quantum computing vulnerabilities. A full description of the methods used is provided in Appendix A.

[2] Confidentiality, integrity, and availability are known as the *CIA triad* in the context of security. Loss of each is defined in 44 U.S.C. § 3552 as follows:

> Loss of Confidentiality: failure to preserve authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
>
> Loss of Integrity: improper information modification or destruction, including loss of assured nonrepudiation and authenticity.
>
> Loss of Availability: Failure to ensure timely and reliable access to and use of information.

Key Definitions

Table 1.1 provides definitions of several key terms used in this report. These definitions are adapted from those in DHS's *Risk Lexicon*, except where otherwise noted.

Understanding Quantum Computing Vulnerabilities

In addition to understanding the basic definitions of the key terms presented in Table 1.1, it is important to understand the distinctions between different types of quantum computing vulnerabilities because these will be important to the assessments. Vulnerabilities from quantum computing fall into two categories, which are distinguished by the different points in time when risk mitigation must occur (Vermeer and Peet, 2020):

- *Remote authentication vulnerabilities* are those associated with maintaining secure remote access to systems. A system with these vulnerabilities must be moved to PQC before an adversary with a quantum computer attacks it. Put another way, the risk to these systems is null until a CRQC exists because there is negligible likelihood that a successful attack on the cryptographic system could occur before then, and the risk could be completely mitigated by adopting PQC.
- The second vulnerability category is referred to as *catch and exploit*. Organizations are currently communicating information using cryptography that is safe now against conventional computers but will not be safe against future quantum computers. An adversary might capture (*catch*) this information now in encrypted form and hold it until a quantum computer exists that can decrypt it (*exploit*). The risk from these catch-and-exploit vulnerabilities therefore depends on how long the information must remain confidential, and risk can accumulate the longer sensitive data are routinely transmitted before adopting PQC in communications. Implementing PQC in communications merely stops risk from accumulating further; it does not eliminate the risk already incurred from allowing an adversary the opportunity to capture valuable information for later decryption.

Remote authentication vulnerabilities would allow an attacker to carry out a wide variety of malicious activities on a compromised system (e.g., theft, data corruption or destruction, file encryption). As a result, these vulnerabilities generally facilitate much more-devastating impacts on systems than catch and exploit does should they not be mitigated before an attack, but there is more time to fix them. For this reason, catch-and-exploit risks will tend to require much more-urgent attention where information with a long confidentiality lifetime is involved.

TABLE 1.1
Definitions of Key Terms

Term	Definition
Confidentiality lifetime	The duration of time that sensitive information remains sensitive and must remain secure (based on Mosca's theorem) (Mosca, 2018, p. 1)
Impact	The effect that can be expected when a given event or incident occurs (*Risk Lexicon*, p. 10)[a]
Risk	The potential for an adverse outcome assessed as a combination of the impact of an event and the likelihood that event will occur (*Risk Lexicon*, p. 27)
Threat	An individual or action that has the potential to cause harm (*Risk Lexicon*, p. 36)
Vulnerability	A "physical feature or . . . attribute that renders an entity, asset, system, network, or geographic area open to exploitation" (*Risk Lexicon*, p. 38)

[a] This definition was adapted from the definition of *consequence*.

Overview of Assessment Steps

Table 1.2 summarizes the key steps in our assessment of the NCFs. These steps are described in detail in Appendix A.

Structure of the Assessment Form

Each NCF assessment form leads with a table summarizing our assessment for the NCF in the categories of urgency, scope, cost, and other factors, followed by the assessment of the priority for assistance to the NCF based on the rankings in those categories. The final entry in the summary table describes the bottom line up front for the assessment: the primary concern or concerns among the issues affecting the NCF. These concerns can include the vulnerabilities and consequences of greatest potential concern to the NCF. In cases in which there is not an NCF-specific vulnerability or consequence, the NCF's primary concern will be to focus on ensuring that it is taking action to prepare for PQC in a timely manner.

This summary is followed by a synopsis that provides context on the primary issues affecting the NCF. In general, the synopsis first presents issues associated with catch-and-exploit vulnerabilities for the NCF, then discusses issues associated with the categories of authentication vulnerabilities described above. The issues discussed in the synopsis are used as the basis for the ratings of urgency, scope, cost, and other factors. Those ratings are then used as justification for the assessment of the NCF's priority for assistance.

Organization of This Report

The remainder of this report is organized as follows: Chapter Two presents the results of the analysis of quantum vulnerabilities, and Chapter Three presents the conclusions. Appendix A describes the methods used to conduct the assessments. Appendix B, which contains the assessments for the 55 NCFs, is available at www.rand.org/t/RRA1367-6.

TABLE 1.2
Overview of Steps for Assessing Quantum Vulnerabilities of National Critical Functions

Step	Approach and Data Source
Identify the relevant information systems and sensitive data that the NCF uses.	Use literature and other data sources, including prior reports, IT literature, market surveys, sector-specific data, and databases describing supply chain relationships.
Identify relevant quantum computing vulnerabilities.	Use context from previous RAND work on the topic and PQC migration demonstration scenarios from NIST.
Rate the urgency of addressing the NCF's vulnerabilities.	Assess the confidentiality lifetime of data that the NCF handles and potential long-term challenges in migrating systems to PQC.
Rate the scope of the organizations and systems requiring updates.	Approximate the number of organizations that must act, based on open literature, industry data, and analysis of affected systems.
Rate the relative cost per organization required to address the vulnerabilities.	Perform a high-level assessment of the extent of software and hardware changes that are likely needed to mitigate vulnerability.
Identify other factors that could make the challenges more or less difficult to address.	Identify other qualitative factors that could make the migration to PQC more or less challenging for the NCF.
Rank the NCF's priority for assistance.	Combine the ratings in all previous categories.

CHAPTER TWO

Assessments of Quantum Vulnerabilities of the National Critical Functions

Using the criteria described in the methodology presented in Appendix A, we assessed the quantum computing vulnerabilities of each of the 55 NCFs. The assessment for each of the NCFs can be found online in Appendix B. In this chapter, we discuss our findings for the full set of 55 NCFs.

Ratings for Urgency, Scope, Cost, Other Factors, and Priority for Assistance

Table 2.1 shows a description of each of the rating categories (urgency, scope, cost, other factors, and priority for assistance; described in more detail in Appendix A), and Table 2.2 shows the ratings assessed for each NCF in these categories. As noted in Table 1.2 in Chapter One, we based our priority ratings on the collected ratings assessed in the other categories (urgency, scope, cost, and other factors). Using this approach, we rated 34 of the NCFs as low priority for assistance, 15 as medium priority for assistance, and six as high priority for assistance.

Although nearly every assessment addressed issues unique to that NCF, many NCFs fall into categories based on notable commonalities. We identified three of the NCFs as critical enablers of the PQC migration for the rest of the NCFs:

- NCF 3, Provide Internet Based Content, Information, and Communication Services
- NCF 35, Provide Identity Management and Associated Trust Support Services
- NCF 52, Provide Information Technology Products and Services.

TABLE 2.1
Descriptions of Rating Categories

Rating	Definition
Urgency	Assessment of how quickly NCF stakeholders must address identified vulnerabilities
Scope	Assessment of how many organizations must take NCF-specific actions to address vulnerabilities
Cost	Assessment of the cost per organization to take NCF-specific actions
Other factors	Assessment of other qualitative factors that could exacerbate or mitigate the challenges the NCF faces in mitigating quantum computing vulnerabilities
Priority for assistance	Combination of the ratings from each of the previous categories; intended to provide a rough categorization of high-, medium-, and low-priority NCFs

TABLE 2.2

Assessments of Quantum Computing Vulnerabilities of the National Critical Functions

Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
Connect						
1	Operate Core Network	Low	Low	Low	Mitigating	Low
2	Provide Cable Access Network Services	Low	High	High	Mitigating	Medium
3	Provide Internet Based Content, Information, and Communication Services	High	High	Medium	Exacerbating	High
4	Provide Internet Routing, Access, and Connection Services	Low	Low	Low	Mitigating	Low
5	Provide Positioning, Navigation, and Timing Services	Low	Low	Low	Neutral	Low
6	Provide Radio Broadcast Access Network Services	Low	Low	Low	Neutral	Low
7	Provide Satellite Access Network Services	High	Medium	Low	Mitigating	Medium
8	Provide Wireless Access Network Services	High	High	Medium	Mitigating	Medium
9	Provide Wireline Access Network Services	Low	High	High	Mitigating	Medium
Distribute						
10	Distribute Electricity	Medium	High	High	Neutral	High
11	Maintain Supply Chains	Low	Low	Low	Neutral	Low
12	Transmit Electricity	Low	High	Low	Mitigating	Low
13	Transport Cargo and Passengers by Air	Medium	Medium	Medium	Mitigating	Medium
14	Transport Cargo and Passengers by Rail	Medium	Low	Low	Mitigating	Low
15	Transport Cargo and Passengers by Road	Medium	Low	Low	Mitigating	Low
16	Transport Cargo and Passengers by Vessel	Medium	Low	Low	Mitigating	Low
17	Transport Materials by Pipeline	Low	Low	Low	Exacerbating	Low
18	Transport Passengers by Mass Transit	Medium	Low	Low	Mitigating	Low
Manage						
19	Conduct Elections	Low	Medium	Low	Exacerbating	Medium
20	Develop and Maintain Public Works and Services	Low	Low	Low	Neutral	Low
21	Educate and Train	Low	High	Low	Neutral	Medium
22	Enforce Law	High	High	Low	Mitigating	Medium
23	Maintain Access to Medical Records	High	Medium	Low	Mitigating	Medium
24	Manage Hazardous Materials	Low	Low	Low	Mitigating	Low
25	Manage Wastewater	Low	Low	Low	Mitigating	Low
26	Operate Government	Medium	High	Low	Exacerbating	Medium
27	Perform Cyber Incident Management Capabilities	Low	Low	Low	Mitigating	Low
28	Prepare for and Manage Emergencies	Low	Low	Low	Neutral	Low

Table 2.2—Continued

Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
29	Preserve Constitutional Rights	Low	Low	Low	Neutral	Low
30	Protect Sensitive Information	High	High	High	Neutral	High
31	Provide and Maintain Infrastructure	Low	Low	Low	Neutral	Low
32	Provide Capital Markets and Investment Activities	Medium	Low	Low	Exacerbating	Medium
33	Provide Consumer and Commercial Banking Services	Low	Low	Low	Neutral	Low
34	Provide Funding and Liquidity Services	Medium	Low	Low	Exacerbating	Medium
35	Provide Identity Management and Associated Trust Support Services	Medium	High	Low	Mitigating	Medium
36	Provide Insurance Services	Medium	Low	Low	Mitigating	Low
37	Provide Medical Care	Low	Low	Low	Neutral	Low
38	Provide Payment, Clearing, and Settlement Services	Low	High	Medium	Mitigating	Medium
39	Provide Public Safety	Low	Low	Low	Mitigating	Low
40	Provide Wholesale Funding	Low	Low	Low	Neutral	Low
41	Store Fuel and Maintain Reserves	Low	Low	Low	Exacerbating	Low
42	Support Community Health	High	Medium	Low	Mitigating	Medium
Supply						
43	Exploration and Extraction of Fuels	Medium	Low	Low	Exacerbating	Low
44	Fuel Refining and Processing Fuels	Medium	Low	Low	Exacerbating	Low
45	Generate Electricity	Medium	High	High	Neutral	High
46	Manufacture Equipment	Medium	Low	Low	Neutral	Low
47	Produce and Provide Agricultural Products and Services	Medium	Low	Low	Mitigating	Low
48	Produce and Provide Human and Animal Food Products and Services	Medium	Low	Low	Mitigating	Low
49	Produce Chemicals	Medium	Low	Low	Mitigating	Low
50	Provide Metals and Materials	Medium	Low	Low	Neutral	Low
51	Provide Housing	Medium	Low	Low	Neutral	Low
52	Provide Information Technology Products and Services	High	High	High	Neutral	High
53	Provide Materiel and Operational Support to Defense	High	High	High	Neutral	High
54	Research and Development	Medium	Low	Low	Neutral	Low
55	Supply Water	Low	Low	Low	Mitigating	Low

Many NCF assessments exhibited similarities based on, for example, their rating of high urgency or their dependence on integrated IT and industrial control systems (ICSs). These groups of NCFs and other notable issues are discussed in the following section.

Categorizing National Critical Functions

Several useful categories arise from the ratings and context provided for each of the NCFs.

Critical Enablers of the Migration to Post-Quantum Cryptography

Three NCFs, shown in Table 2.3, were identified as critical enabling functions for the broader migration to PQC among the rest of the NCFs. That is, these are the NCFs on which nearly every other NCF depends to provide the tools needed to mitigate quantum computing vulnerabilities. Specifically, these NCFs are the ones most responsible for providing the products and services that use public-key cryptography to protect sensitive information in networked environments, especially those functions that are facilitated by the Internet in some way. The products and services provided by NCFs 3 and 52 are typically those that perform the public-key encryption operations used to secure data and communications, and NCF 35 is responsible for issuing and managing the digital certificates that form a cornerstone of identity management and authentication in networked environments.

Although many organizations responsible for other NCFs will need to take specific, occasionally unique, actions to effect a migration to PQC in their own operations, they will often be able to do so only if these three NCFs create the updated products and services that enable those actions. An organization with a presence on the Internet can migrate its website to PQC, for example, only if the software and web server hardware it uses have been updated to allow configurations using post-quantum algorithms and it can install a post-quantum digital certificate. If it engages in e-commerce, it might also need third-party payment service providers to perform updates. If it requires workers to be able to remotely access its internal network, it needs to be able to configure virtual private network (VPN) applications to use PQC. Finally, it will be able to prohibit the option to interact with others using current, vulnerable cryptographic methods only once enough of the ecosystem of customers and partners has also migrated to the point that very few organizations do not have PQC configurations enabled.

The broader migration to PQC in networked environments that will enable that final state, in which nearly every system is interoperable using PQC, cannot effectively begin until NCFs 3, 35, and 52 produce the products and services that make it possible. These NCFs will require a broad scope of organizations to act quickly, often at significant expense. If organizations responsible for these NCFs do not act quickly to migrate affected products and services to incorporate the PQC standard, other NCFs will not have the tools

TABLE 2.3
Critical Enablers of the Migration to Post-Quantum Cryptography

Category	Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
Connect	3	Provide Internet Based Content, Information, and Communication Services	High	High	Medium	Exacerbating	High
Manage	35	Provide Identity Management and Associated Trust Support Services	Medium	High	Low	Mitigating	Medium
Supply	52	Provide Information Technology Products and Services	High	High	High	Neutral	High

to address quantum computing vulnerabilities in their own operations. As a result, these organizations represent critical dependencies for the other NCFs in addressing vulnerabilities to quantum computing. Our ratings for the other NCFs assume that these critical enablers will provide the tools in a timely manner. If it becomes clear over time that this will not be the case, the vulnerabilities and risks would become much more significant nearly uniformly across the rest of the set of NCFs. CISA should prioritize monitoring the progress of these NCFs in producing the products and services needed to facilitate the migration to PQC. It was beyond the scope of this study to describe a complete assessment of the key migration milestones to monitor in these NCFs. However, such an assessment would likely include key examples, such as the ability to configure enterprise software products to use PQC in key exchange, the release of a quantum-resistant version (or replacement) of TLS, and the issuance of quantum-resistant digital certificates.

High Priorities for Assistance

Six NCFs, shown in Table 2.4, were categorized as high priority for assistance.

NCFs 3 and 52 were rated as high priority primarily because they are likely to be two of the most-important critical enablers of the PQC migration for the rest of the NCFs, as discussed previously. They will need to prioritize the provision of products and services that enable others to migrate to PQC, and this will likely require a very large number of organizations to act quickly to develop solutions that will meet the varied requirements of customers in an interoperable way. This is likely to be a highly complex and costly task for many affected organizations, depending on the application.

A NIST project is underway that intends to assess the scale and complexity of this task for various applications (Barker, Souppaya, and Newhouse, 2021), and DHS has created a roadmap of steps that critical infrastructure organizations should be taking now to prepare for the PQC migration (DHS, 2021). Although many organizations responsible for these NCFs have been actively engaged for some time in preparing for the PQC migration (Campagna and Crockett, 2021; Cimpanu, 2021; Crane, 2020; FutureTPM, undated; Kwiatkowski and Valenta, 2019; Mitchell, 2020; Pala, 2020; Paquin, Stebila, and Tamvada, 2020; TCG, 2020; Weibel, 2020) and are unlikely to need technical assistance, these NCFs cover a diverse ecosystem of providers with varying characteristics and needs. These NCFs will continue to benefit from government coordination and standardization efforts, and many organizations will likely benefit from ongoing efforts across government to help them prepare for the PQC migration.

NCF 30, Protect Sensitive Information, is in many ways an unstated subfunction within each of the other NCFs. Because the rest of the NCFs depend so much on NCFs 3, 35, and 52 to help them protect sensitive

TABLE 2.4
National Critical Functions Rated High Priority for Assistance

Category	Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
Connect	3	Provide Internet Based Content, Information, and Communication Services	High	High	Medium	Exacerbating	High
Distribute	10	Distribute Electricity	Medium	High	High	Neutral	High
Manage	30	Protect Sensitive Information	High	High	High	Neutral	High
Supply	45	Generate Electricity	Medium	High	High	Neutral	High
Supply	52	Provide Information Technology Products and Services	High	High	High	Neutral	High
Supply	53	Provide Materiel and Operational Support to Defense	High	High	High	Neutral	High

information (in the context of quantum computing vulnerabilities), the ratings given in each category for NCF 30 are derived largely from a combination of the factors that influenced the assessments for those three NCFs. The assessed urgency, scope, and cost are therefore high for NCF 30 for the same reasons they are high in the three critical enabling NCFs, and this resulted in a rating of high priority.

NCFs 10, Distribute Electricity, and 45, Generate Electricity are rated as high priority primarily because of the uniquely challenging operational requirements and complexity of electricity distribution.[1] Like many other NCFs, electricity generation and distribution operations depend heavily on connected ICS technology. These NCFs have specific issues, however, that make them more challenging than other ICS-dependent NCFs, especially

- wide geographic dispersion of ICS technologies
- strict requirements for secure real-time monitoring and control of some operational technology with low communication latency
- heterogeneous regulatory requirements and technology standards.

Additionally, per Keith Stouffer and his colleagues, "Electric power is often thought to be one of the most prevalent sources of disruptions of interdependent critical infrastructures" (Stouffer et al., 2015, p. 2-3). These challenges led to assessments of broader scope and higher cost of migration for these NCFs than for many other highly ICS-dependent NCFs. Owners and operators, technology vendors, regulatory authorities, and standard-setting bodies in these NCFs might therefore be in more need of assistance in support of the migration to PQC.

The final NCF in this group, 53, Provide Materiel and Operational Support to Defense, is rated as high priority largely because of the high sensitivity of information it handles, the long confidentiality lifetime of those data, and the high likelihood that this NCF will be a target for well-resourced threat actors. A significant amount of classified and sensitive-but-unclassified data in this NCF is often in transit. Transmitting these data requires protection by public-key cryptography algorithms, which are vulnerable to quantum computing and therefore represent a catch-and-exploit vulnerability. The scope of affected organizations is broad, and, although costs can vary considerably from one organization and application to another, they are likely to be high overall. We identified the potential for this NCF to be a target for a nation-state adversary as a significant exacerbating factor, although the NCF will benefit from the significant central authority of the National Security Agency/Central Security Service (NSA/CSS) in dictating cybersecurity requirements for commercial national security systems (see Committee on National Security Systems, 2016, and NSA/CSS, 2015).

High-Urgency National Critical Functions

We rated nine NCFs as high urgency (Table 2.5). In every case, we gave this rating primarily because the NCF handled data with a long confidentiality lifetime and therefore experienced a significant catch-and-exploit vulnerability.

We identified only three categories of data that had sufficient sensitivity and long-enough confidentiality lifetime to justify this rating: protected health information (PHI), data used by the justice system (especially such data as witness or informant identities), and national security data. We rated NCFs 3, 7, 8, 30, and 52

[1] Some electricity generation sources, especially distributed energy resources, are closely logically integrated with electricity distribution technology and operations. NCFs 10 and 45 therefore share many of the same characteristics that led to the assessed ratings in each category. NCF 12, Transmit Electricity, in contrast, has notable differences from these two NCFs in both regulatory environment and relevant technology issues.

TABLE 2.5
National Critical Functions Rated High Urgency

Category	Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
Connect	3	Provide Internet Based Content, Information, and Communication Services	High	High	Medium	Exacerbating	High
Connect	7	Provide Satellite Access Network Services	High	Medium	Low	Mitigating	Medium
Connect	8	Provide Wireless Access Network Services	High	High	Medium	Mitigating	Medium
Manage	22	Enforce Law	High	High	Low	Mitigating	Medium
Manage	23	Maintain Access to Medical Records	High	Medium	Low	Mitigating	Medium
Manage	30	Protect Sensitive Information	High	High	High	Neutral	High
Manage	42	Support Community Health	High	Medium	Low	Mitigating	Medium
Supply	52	Provide Information Technology Products and Services	High	High	High	Neutral	High
Supply	53	Provide Materiel and Operational Support to Defense	High	High	High	Neutral	High

as high urgency because of their function in protecting sensitive customer data that might have a long confidentiality lifetime, even though their own operations do not involve the generation or use of data with a long confidentiality lifetime. NCF 22 handles sensitive justice system data, NCFs 23 and 42 handle PHI, and NCF 53 handles national security data.

In rating urgency, we also considered personally identifiable information (PII), personal finance records, and commercial IP and trade secrets, but, in general, these data categories were expected to only have medium or short confidentiality lifetimes (i.e., less than ten years). PII is typically considered sensitive because it is used in knowledge-based verification mechanisms, in which someone can prove their identity to another party by providing personal information that only that individual is likely to know. The identity management ecosystem is constantly evolving, however, and there appears to be widespread recognition that knowledge-based verification schemes based on aggregated personal data are increasingly inadequate (Better Identity Coalition, 2018; Commission on Enhancing National Cybersecurity, 2016; Grassi, Garcia, and Fenton, 2017). Many attributes used for identity verification will not have long validity lifetimes (e.g., home address), while other attributes with long validity lifetimes (e.g., social security number) could be phased out of use in identity verification (Better Identity Coalition, 2018). Given this context, PII is not considered to have a long confidentiality lifetime, although certain attributes might have moderate confidentiality lifetimes (i.e., one to ten years). Industry trade secrets were also expected to have a moderate confidentiality lifetime in most cases. Some industries might have trade secrets with unusually long confidentiality lifetimes (e.g., pharmaceuticals and defense industrial base organizations), but it is likely that most are less than ten years (Defense Security Service, 2013).[2] It is also likely that many trade secrets are kept within internal networks and only rarely transmitted in a way that would make them vulnerable to catch and exploit. The practical challenges associated with carrying out a significant catch-and-exploit campaign and the moderate confidentiality lifetime of PII and trade secrets typically resulted in a rating of medium urgency for NCFs that handled these data.

[2] These issues are discussed in further detail in the assessment of NCF 54, Research and Development.

Industrial Control System–Dependent National Critical Functions

In 18 of the NCF assessments, we identified dependence on ICS technology as a significant defining characteristic of the NCF's quantum computing vulnerabilities (Table 2.6). Although some of these NCFs also have other concerns (e.g., some NCFs exhibit catch-and-exploit vulnerabilities with respect to trade secrets), the assessments for these NCFs are otherwise defined largely by the quantum computing vulnerabilities that arise from organizational use of integrated IT and ICS architectures.

Integrated ICSs often face significant cybersecurity vulnerabilities as industries replace legacy operational hardware with digital devices, and monitoring and control of these devices are integrated with other business IT systems. Per the ICS-CERT, "[m]odern control system architectures, business requirements, and cost control measures result in increasing integration of corporate and ICS IT architectures" (ICS-CERT, 2016, p. 1). As part of the security policy for those networks, PKI and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (ICS-CERT, 2016; Stouffer et al., 2015).

Although the use of public-key cryptography–based security mechanisms will create quantum computing vulnerabilities where they are used in these networked systems, deployed ICS technology is often resource-

TABLE 2.6

National Critical Functions with Vulnerabilities Significantly Defined by the Use of Industrial Control Systems

Category	Number	Name	Urgency	Scope	Cost	Other Factors	Priority for Assistance
Distribute	10	Distribute Electricity	Medium	High	High	Neutral	High
Distribute	12	Transmit Electricity	Low	High	Low	Mitigating	Low
Distribute	14	Transport Cargo and Passengers by Rail	Medium	Low	Low	Mitigating	Low
Distribute	16	Transport Cargo and Passengers by Vessel	Medium	Low	Low	Mitigating	Low
Distribute	17	Transport Materials by Pipeline	Low	Low	Low	Exacerbating	Low
Distribute	18	Transport Passengers by Mass Transit	Medium	Low	Low	Mitigating	Low
Manage	24	Manage Hazardous Materials	Low	Low	Low	Mitigating	Low
Manage	25	Manage Wastewater	Low	Low	Low	Mitigating	Low
Manage	41	Store Fuel and Maintain Reserves	Low	Low	Low	Exacerbating	Low
Supply	43	Exploration and Extraction of Fuels	Medium	Low	Low	Exacerbating	Low
Supply	44	Fuel Refining and Processing Fuels	Medium	Low	Low	Exacerbating	Low
Supply	45	Generate Electricity	Medium	High	High	Neutral	High
Supply	46	Manufacture Equipment	Medium	Low	Low	Neutral	Low
Supply	47	Produce and Provide Agricultural Products and Services	Medium	Low	Low	Mitigating	Low
Supply	48	Produce and Provide Human and Animal Food Products and Services	Medium	Low	Low	Mitigating	Low
Supply	49	Produce Chemicals	Medium	Low	Low	Mitigating	Low
Supply	50	Provide Metals and Materials	Medium	Low	Low	Neutral	Low
Supply	55	Supply Water	Low	Low	Low	Mitigating	Low

constrained. These resource constraints influence the security mechanisms used in deployed ICS devices, especially with respect to computationally demanding algorithms associated with public-key cryptography (i.e., complex authentication is often difficult to implement because these technologies have limited onboard memory and computing power compared with other IT systems). Per Stouffer and his colleagues,

> ICS and their real time [operating systems] are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems are often lacking resources common on modern IT systems. Many systems may not have desired features including encryption capabilities, error logging, and password protection. Indiscriminate use of IT security practices in ICS may cause availability and timing disruptions. There may not be computing resources available on ICS components to retrofit these systems with current security capabilities. (Stouffer et al., 2015, p. 2-15)

Industries often opt to use less vulnerable cryptographic security mechanisms (e.g., preshared symmetric keys or hashing algorithms) in some operational technology because they require fewer computational resources (Stouffer et al., 2015). That being said, where quantum computing vulnerabilities do exist in deployed ICS architectures, addressing them could be challenging and costly. Modern digital ICS devices often have operational lifetimes that range from three to five years, and they will likely be replaced with PQC-compatible devices (where applicable) during planned hardware refreshes, but some devices custom-made for specific uses can have operational lifetimes of ten to 15 years or more. Furthermore,

> [s]oftware updates on ICS cannot always be implemented on a timely basis. These updates need to be thoroughly tested by both the vendor of the industrial control application and the end user of the application before being implemented . . . . Many ICS utilize older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable. (Stouffer et al., 2015, p. 2-15)

Given these factors, assessing the importance of quantum computing vulnerabilities in integrated ICSs is a complex task. Quantum computing vulnerabilities might not be a factor at all where ICS devices do not use cryptography or where they already use quantum-resistant methods (e.g., symmetric keys used in wireless communications). Many modern devices that do depend on public-key cryptography can likely be replaced with PQC-compatible versions during planned hardware refreshes. Furthermore, networked ICSs often also rely on additional, layered network security mechanisms that would further mitigate vulnerability (*defense in depth*), even where long-lived operational technologies were deployed with vulnerable cryptographic security mechanisms (ICS-CERT, 2016).

If organizations quickly begin to follow the preparatory steps in the DHS roadmap for the migration to PQC and integrate risk to ICS networks from quantum computing vulnerabilities into other cybersecurity risk management and defense-in-depth strategies, the migration to PQC could be very manageable for many ICS-dependent organizations. Software being deployed in the next few years can incorporate the cryptographic agility to accommodate PQC and future cryptographic transitions, and most operational technology can be replaced with compatible versions during planned hardware refreshes. This is expected to be the case for most of the NCFs in this category (again, assuming that the appropriate vendors in NCFs 3 and 52 quickly make the necessary products and services available for implementation).

However, in applications in which all of the above factors are inadequate to mitigate risk and deployed ICS technology leaves an unacceptable quantum computing vulnerability, addressing it could be a challenging and costly task. Indeed, the increased computational demands of PQC algorithms compared with those of current public-key cryptography algorithms could make the PQC migration very complex and costly, especially in industries in which ICS networks are geographically dispersed and networks require secure, real-time, low-latency monitoring and control of devices. Electricity distribution is one such application.

CHAPTER THREE

Key Findings and Conclusion

In this chapter, we present our key findings and conclude the report.

Key Findings

All NCFs will need to prepare for the migration to PQC, even those that received low ratings in the assessments. Low ratings in the NCF assessments do not imply that NCF owners, operators, and other stakeholders have no need to pay attention to this issue. On the contrary, the vulnerabilities created by quantum computing are as far-reaching as the Internet, and every single NCF will be affected in some way. The ratings given in the NCF assessments are largely intended to provide context and a point of comparison for government stakeholders as they consider how and where to focus outreach to the NCFs. If every NCF organization that needed to address the PQC migration in some way were included in the rating for scope in the assessments, that rating would always be high, and the rating would lose its utility in the assessment.

Every NCF organization should begin to follow the steps outlined in the DHS roadmap for PQC migration and should do so soon, even before the completion of the NIST PQC standardization project. Beyond simply preparing for the migration to PQC, organizations should take steps to build resilience by also preparing for the cryptographic transitions that will come next. The security afforded by any implementation of encryption is not static—it diminishes over time as computational capability and technique advance. Cryptographic keys that were widely used decades ago would provide woefully inadequate security today, and the forthcoming PQC standard will also one day be replaced. Designing information systems so that they can easily adapt to support future changes to cryptography standards is a concept known as *cryptographic agility*, and it is a significant focus in NIST's broader effort to support the migration to PQC (Barker, Souppaya, and Newhouse, 2021). Every organization, regardless of the urgency with which it approaches quantum computing vulnerabilities, should begin to consider how it can embed technology and practices that support cryptographic agility as a way to improve overall cybersecurity.[1]

When following the steps in the DHS roadmap for PQC migration, some NCF stakeholders might ultimately assess that the migration will largely happen invisibly for them, with little active intervention. In the assessments for some NCFs, we concluded that vulnerabilities arose primarily from a reliance on Internet-connected IT, and we identified few other specific issues of importance. In these cases, stakeholders can expect that commonplace software applications, such as web browsers and email software, will eventually be updated to enable configurations that use PQC algorithms. These organizations will nevertheless need to inventory where quantum computing vulnerabilities might arise for them, confirm that responsibility for updates will fall on vendors, identify any configuration changes they will need to make, and ensure that

[1] See Forum on Cyber Resilience, 2017, for a more in-depth resource on planning for cryptographic agility as a way to build cyber resilience.

no further IT transformation plans are necessary. Other NCFs will need to take similar steps (often much broader in scope), regardless of the ratings they received.

Although NCF 27, Perform Cyber Incident Management Capabilities, will not experience any unique vulnerabilities itself, it will have a pivotal role in providing early preparation and prevention efforts for other NCFs. Stakeholders in the NCF should plan to start helping customers understand and prevent any catch-and-exploit vulnerabilities, and incident management stakeholders should encourage customers to inventory their vulnerabilities (especially public-key cryptography use) in preparation for the migration to PQC. Early intervention by incident managers and prevention efforts in this NCF will aid more broadly in making sure NCFs get a robust start to the migration that will not leave lingering authentication vulnerabilities once a quantum computer arrives.

On this issue, we also note in conclusion that organizations often delay IT modernization and life-cycle replacement of hardware long after systems are considered obsolete. With this in mind, even NCFs that received low ratings in most categories might exhibit significant vulnerabilities in the future if they do not eventually perform the necessary updates to enterprise IT and other relevant information systems. CISA should plan to reassess the state of quantum vulnerabilities in the NCFs once the PQC migration is well underway to identify where failures to update obsolete technology could create persistent vulnerabilities.

Completely addressing quantum computing vulnerabilities will require that most stakeholders in each NCF adequately adopt PQC, but much of the vulnerability can be quickly addressed if relatively few key entities prioritize the migration. At many points in communication infrastructure, quantum computers will create vulnerabilities, and each of these eventually needs to be inventoried and addressed. Addressing quantum computing vulnerabilities will require coordinated action across all the NCFs. However, we identified three NCFs as critical enablers for the PQC migration. This is because, although every NCF stakeholder will need to take action of some kind, a significant portion of the vulnerabilities across the NCFs can be addressed by relatively few actions by major stakeholders within these NCFs.

New post-quantum versions of common communication protocols and standards will need to be developed and released. Post-quantum versions of, for example, TLS, Internet protocol security (IPsec), Secure/Multipurpose Internet Mail Extensions (S/MIME), and digital certificates will be needed. At first, many such examples will need to use a hybridization of conventional and PQC algorithms. Once these standards are released, a few major stakeholders will need to update products and services to enable the use of the standards. For example, web browsers and cloud service providers might need to update software to support a post-quantum version of TLS; email applications will need to update to support a post-quantum version of S/MIME; and certificate authorities will need to make post-quantum digital certificates available. These are likely to involve complex changes that many stakeholder organizations are already considering and testing.

After these steps occur, however, other organizations can begin to perform the thousands of configuration changes, software rewrites, hardware updates, and reissuing of certificates that will constitute the majority of the broader migration to PQC across the NCFs. At that point, the use of PQC will be *possible*, even if it is not yet *enabled by default* or the only allowed option for networked communications. Although the assessments detail many scenarios in which specific issues will still be challenging and costly for some NCF stakeholders, organizations that must address urgent catch-and-exploit vulnerabilities will have the tools to do so, and the challenges associated with the migration can be integrated into broader change management planning for business IT and relevant ICSs. Furthermore, evidence from previous transitions suggests that many organizations adopt a new standard within a few years, even if there is a long waiting period before nearly everyone effects the migration ("Apple," 2018; Salowey, Turner, and Wood, 2019).[2]

[2] For example, 27 to 30 percent of observed web connections from major web browser applications used the TLS 1.3 standard within a year of its release. See Salowey, Turner, and Wood, 2019.

Assessments of the NCFs (especially in the Connect category) elucidate how encryption is used in many different, often overlapping, ways in information and communication infrastructure. Data can be encrypted in storage on a user's device. Messages sent across the Internet can be encrypted in secure connections (e.g., using TLS) established through web browsers, email applications, and other software. The traffic in the wireless link between a user device and the local wireless access point (e.g., a Wi-Fi router) is encrypted again with a symmetric key. Data are decrypted by the router, then often sent to cable network access points (i.e., cable modems), where traffic is encrypted on the wired cable network. If satellite networks are used, the wireless links between satellites and ground segments are often encrypted. Internet routing infrastructure does not further encrypt the data, but the requests to the routing systems are often authenticated with PKIs.

What we found was that many NCFs had responsibility for just a single link each in these chains. We identified issues they needed to consider to address any quantum computing vulnerabilities in those links (e.g., incorporating PQC in security for the border gateway protocol or increasing symmetric-key strength in wireless links). But no stakeholders, even those in the Connect category, are acting in isolation, and many potential vulnerabilities would ultimately be minor issues if vulnerabilities were addressed in key places elsewhere. For example, cable network access providers might need to begin using stronger symmetric keys in hardware to adequately protect traffic on their networks, but if 99 percent of the traffic on their networks were already using a post-quantum TLS connection or a VPN facilitating a post-quantum version of IPsec, those weak symmetric keys would be unlikely to pose a significant vulnerability.

Practical challenges with executing catch-and-exploit campaigns mean that very few NCFs likely need to urgently address catch-and-exploit vulnerabilities, although many functions will exhibit them. Many NCFs will exhibit catch-and-exploit vulnerabilities. Organizations communicate encrypted data containing PII, industrial trade secrets, PHI, sensitive justice system information, and national security data. These data might occasionally have very long confidentiality lifetimes (i.e., more than ten years), and an adversary that captures these encrypted communications now would be able to reveal their contents once in possession of a CRQC that could derive the secret key used to encrypt them. However, although this possibility is worrisome in principle, consider the practical challenges associated with carrying out such a campaign in practice:

- An adversary must be able to intercept encrypted communications. This would be more challenging for wired networks than for wireless signals, although there are many ways to accomplish this even on wired networks with physical security.
- A potentially very sizable amount of captured data would need to be stored for years—possibly a decade or more.
- An adversary would likely have few indications of what the contents of any specific communications were until they were decrypted. Adversaries might be able to infer the potential value of the data based on metadata, such as size, time of transmission, and which endpoints were communicating, but they would have few other useful ways to identify which communications should be prioritized for decryption.
- Decrypting communications could involve the derivation of many cryptographic keys. Depending on the scenario, a single key could reveal a large amount of data (if, for example, the key was expected to provide long-term security) or a small amount of data (if, for example, the key was ephemeral and used only for a single connection).
- Finally, every key derivation will likely require a considerable level of effort, potentially involving teams of personnel and a device working for days or weeks at a time. As the technology matures, devices might proliferate, and this level of effort would decrease, but it could be years after the first CRQC breaks a key before it becomes a relatively trivial task to do so.

Given these practical difficulties, it will likely be a tremendous challenge for an adversary to carry out a long-term catch-and-exploit campaign. Only a very well-resourced adversary (e.g., a technologically advanced nation-state) would likely expect to be among the first to have the necessary technology and have the foresight needed to execute such a campaign. Even then, it would likely attempt a long-term campaign only on targets that would be seen as very high value.

Every NCF stakeholder that transmits sensitive data will need to implement PQC for key exchange to prevent this vulnerability, but it is likely that only a few NCFs need to truly approach the matter with urgency. PII, industry trade secrets, and other data with moderate to short confidentiality lifetimes are unlikely to be targets of a long-term catch-and-exploit campaign. Although PHI data have a very long confidentiality lifetime, the practical utility of the data to a threat actor capable of carrying out a campaign like this is likely low.

Some very sensitive justice system data (discussed in more depth in the assessment for NCF 22, Enforce Law) might be realistic targets for a catch-and-exploit campaign, but we consider the issue to be most pertinent to organizations responsible for NCF 53, Provide Materiel and Operational Support to Defense. National security–related data handled by organizations responsible for this NCF both have an exceptionally long confidentiality lifetime and would likely be seen as very high value to potential nation-state adversaries. Some organizations responsible for these two NCFs should consider this a serious vulnerability that must be addressed as soon as it is practical to do so, while most others can likely afford to allow more time to pass before it becomes an urgent matter.

Many factors related to the PQC migration are still unknown or uncertain, and it is not yet clear what elements of the migration will present serious challenges for NCF stakeholders. The final PQC standard has not yet been released. Although many stakeholders have begun to prepare for the migration by experimenting with each of the finalist algorithms, many uncertainties will remain by the time the standard is released. NIST and its partners are beginning efforts to create tools for the discovery and inventory of all instances in which updates will be needed, but, as described by Barker, Souppaya, and Newhouse, 2021,

> There is currently no inventory that can guide updates to standards, guidelines, regulations, hardware, firmware, operating systems, communication protocols, cryptographic libraries, and applications that employ cryptography that meets the need to accelerate migration to quantum-resistant cryptography.

We have tried to identify concrete examples of systems and vulnerabilities that will need attention in each of the NCFs and use a high-level analysis to inform a judgment of priority for assistance. For many affected systems, however, the details will matter, and a high-level analysis such as that carried out for these assessments will overlook many of them. Steps in the transition that were expected to be straightforward and simple will instead be complex problems that do not have easy solutions. Elements of information and communication infrastructure that were expected to be immaterial to migration considerations could end up creating unforeseen incompatibilities and bugs. The NCF assessments are intended to provide insights but are by no means comprehensive; however, they can be used as a guide to identify which NCFs might merit a more thorough analysis, depending on the priorities of the entities seeking to provide assistance.

Conclusion

A CRQC will create significant vulnerabilities for stakeholders providing NCFs. Quantum computing will break a foundational element of current information security architectures in a manner that is categorically different from present cybersecurity vulnerabilities. Fortunately, the NIST PQC standard is likely to provide an effective solution to this problem, but the migration to use this standard across critical infrastructure is likely to be a long, complex, and costly effort.

We performed high-level assessments of how quantum computing cryptography vulnerabilities will affect each of the 55 NCFs identified by DHS. Although there is wide variation in the urgency with which stakeholders must attend to this issue, the scope of affected organizations, and the level of effort each organization will need to expend to address vulnerabilities, every stakeholder providing an NCF will be affected in some way.

A few NCFs will likely be critical enablers for other stakeholders to begin the broader migration to PQC across critical infrastructure. Many NCFs will need to urgently address growing risk from catch-and-exploit vulnerabilities or incorporate PQC into long-term acquisition strategy for operational technology. Even stakeholders responsible for NCFs that received ratings of low priority for assistance should take steps to prepare for the PQC migration in advance of the release of the standard, following steps outlined in the DHS roadmap for the migration. Furthermore, all NCF stakeholders can improve cybersecurity resilience more generally by beginning to incorporate strategies for greater cryptographic agility in overall cybersecurity risk management and IT change management strategies.

The analysis described in this report was performed at a high level to provide the context and justification needed to inform and direct engagements with stakeholders responsible for NCFs. Although this approach was useful in this endeavor, the information and communication architectures used across the NCFs are diverse and complex. Moreover, the algorithms that will be chosen for the final PQC standard are not yet finalized, and many uncertainties remain in planning for the cryptographic transition. A high-level approach will inevitably overlook details that will be consequential for specific stakeholder concerns in the NCFs. This analysis should be followed up by additional work to assess, in detail, the specific challenges that will be faced by many of the stakeholders responsible for NCFs, in consultation with subject-matter experts, government partners, and the private sector.

APPENDIX A

Methods Used in the Assessments

In this appendix, we describe in detail the approach used to assess whether exploited quantum computing vulnerabilities could significantly degrade or disrupt the NCFs. We assessed each of the 55 NCFs individually using the set of NCFs and definitions described in a status update to the critical infrastructure community (CISA, 2020b). In each case, we sought to identify the systems (1) that would use cryptography in some way that would be vulnerable to quantum computing and (2) in which it would be the exclusive purview of the NCF to operate, manage, or provide in support of other NCFs.

The Initial Steps in the Assessment

In this section, we describe the first two steps in the assessment process. The remaining steps are rating and analyzing the five items in the assessments provided in Appendix B, available online.

Identify the Relevant Information Systems and Sensitive Data That the National Critical Function Uses

For each NCF, we first examined literature and databases that provide insight into the information systems and sensitive data relevant to that NCF. Because there was no existing official decomposition of the whole set of NCFs into subfunctions, assets, or components, we used different data sources for each NCF, as needed, to inform the analysis. These data sources included prior reports decomposing subsets of NCFs; literature describing IT challenges for NCFs or industry sectors; market surveys; sector-specific data, such as company information from the North American Industry Classification System (NAICS); and databases describing supply chain relationships (e.g., FactSet) (FactSet, 2021). Two examples are illustrative of this strategy: the assessments for NCF 4, Provide Internet Routing, Access, and Connection Services, and NCF 17, Transport Materials by Pipeline.

For NCF 4, DHS published an IT-sector risk assessment in 2009 (DHS, 2009) and, more recently, a technical report on ongoing attempts to functionally decompose the NCFs (CISA, 2020a). We used these reports, as well as other available literature on the primary protocol used by the NCF to route Internet traffic (see Koukounas, Vytogianni, and Dekker, 2019), to identify the major relevant information systems for the NCF. For NCF 17, however, we found no such literature on the IT systems used by the sector. In this case, in addition to open literature describing pipeline material distribution in the United States (see, for example, Markets and Markets, undated; Nygaard and Mukhopadyay, 2020; Oil and Natural Gas Subsector Coordinating Council, 2018), we identified relevant IT systems, first, by searching for industry data associated with NAICS code 486, Pipeline Transportation of Natural Gas, then, once we had identified the major companies associated with the subcategories of this NAICS code, by searching the FactSet database for companies that supplied software products to many of these companies (FactSet, 2021). Using these data sources, it became clear that the NCF used a variety of software solutions for standard business operations (e.g., email, enterprise resource management), and managing cyber-physical systems associated with control and monitoring

of the pipeline network, but these are software and hardware solutions provided to the NCF, not developed, produced, or updated by the NCF itself.[1]

Identify Relevant Quantum Computing Vulnerabilities

Upon identifying the relevant systems and data used in each NCF, we assessed the major quantum computing vulnerabilities affecting the NCF. When performing these analyses, we relied on context from previous RAND work on the topic (Vermeer and Peet, 2020) and PQC migration demonstration scenarios from NIST (Barker, Souppaya, and Newhouse, 2021).

Modes of Disruption of the National Critical Functions

To facilitate the assessment of vulnerable systems that were the exclusive purview of each NCF, we used a simple, high-level taxonomy of issues caused by quantum computing that could lead to a degradation or disruption of the function. This taxonomy, shown in Table A.1, is based on the well-known security triad of confidentiality, integrity, and availability and the modes by which attacks could disrupt a function as described in the MITRE ATT&CK framework (MITRE, undated):

- A function could be disrupted by a loss of confidentiality so significant that an operator removes access to a critical information resource to prevent the unauthorized revelation or theft of information.
- A function could be disrupted by a loss of integrity if an attacker gained the ability to manipulate data such that legitimate users ceased to use the system because they could no longer trust its accuracy.
- Loss of availability implies that an attacker's actions actively deny the use of the system. This could take the form of, for example, removal of network or account control and removal of the owner's administrative privileges or rendering critical cyber-physical systems physically inoperable in some way.

Classes of Vulnerability

The analysis further distinguished between the two classes of vulnerability: catch and exploit and remote authentication. As discussed in Chapter One, this distinction is based on the urgency of measures to remediate the vulnerability. It is generally critical that action be taken on catch-and-exploit vulnerabilities as soon as possible in order to limit the amount of sensitive information that is available for later decryption. The urgency is greater for information with a long confidentiality lifetime (i.e., ten or more years).[2] Remote authentication vulnerabilities, in contrast, generally require much less urgent remediation actions. Fixes for these vulnerabilities must be in place only before an attacker with a CRQC actually tries to break into a vulnerable system. Although this reduces the urgency of addressing the vulnerability, that does not necessarily imply an automatically lower priority for attention and remediation. If exploited, remote authentication vulnerabilities are likely to lead to substantially larger impacts to functions, and they could be much more widespread or require orders of magnitude more resources to address prior to the date the vulnerability could be actively exploited (Vermeer and Peet, 2020).

[1] NIST defines *cyber-physical systems* as "smart systems that include engineered interacting networks of physical and computational components" (Griffor et al., 2017, p. vi).

[2] The definition of a long confidentiality lifetime as ten years or more is based on analysis found in Vermeer and Peet, 2020, showing that PQC standards would likely be released between 2022 and 2024 and a CRQC was expected to exist in the mid-2030s. According to this framework, an organization that used data with a secrecy lifetime longer than ten years would likely need to implement PQC for transmission of those data as soon as possible after standards were released.

TABLE A.1
Select Quantum Vulnerability Modes of National Critical Functions

		Loss Incurred		
Access Type	Example Impact	Confidentiality	Integrity	Availability
Catch and exploit				
	Sensitive data collection	x		
Remote authentication				
Database access	Sensitive data collection	x		
	Data destruction, corruption, manipulation, or encryption		x	
Network access	Theft or resource hijacking		x	
	Sensitive data collection	x		
	Data destruction, corruption, manipulation, or encryption		x	
	Access removal			x
Cyber-physical system access	Device inoperability, inaccessibility, or damage			x
	Sensitive data collection	x		

We considered three broad categories of remote authentication issues:

- *Database access* refers to access to systems that enable information-sharing and access to data sets that are critical to the function. This would include fingerprint databases used by NCF 22, Enforce Law; voter registration databases used by NCF 19, Conduct Elections; or training material databases used by NCF 21, Educate and Train. In some cases, these data might be very sensitive, and a loss of trust in the security of the systems used to access them could be sufficient to disrupt the function. In others, the main concern might be protecting the integrity and availability of the data set itself. In other words, in some cases, it is crucial that an attacker not be able to fake a general user's authentication to access and *read* information from the database; in others, it is crucial that the attacker not be able to gain administrative privileges for the database that would allow it to *write* or alter bulk data in some way.
- *Network account access* refers to the ability to gain trusted, authenticated control of accounts on a network. This would include impersonating an organization by obtaining its private key, thus allowing trusted uploads of malware disguised as software updates, or the ability to falsely identify oneself as a bank account holder or even a bank itself and request fund transfers.
- *Cyber-physical system access* refers to the ability to remotely access and control physical devices. This would include directing the function or gathering data from ICSs; controlling physical security measures, such as door locks; and a plethora of other devices accessed and controlled over the Internet.

Although these three categories share some similarities (e.g., they could all be thought of as account access in some ways), the distinctions still provide a useful high-level construct for categorizing relevant issues in each NCF. The specific ways the analysis uses these categories will vary from NCF to NCF, depending on what systems the NCF employs and how those systems might be critical to supporting other NCFs. Although there will be some exceptions, in general, the relevant issues for most NCFs will be related to data or processes that are handled at the application or presentation layers of the Open Systems Interconnection model of computer networking because those are the layers that typically handle data encryption (see Cloudflare, undated b).

Assessing Ratings in Each Category

Rate the Urgency of Addressing Each National Critical Function's Vulnerabilities

We first assessed urgency—that is, how important it will be for an NCF to address vulnerabilities sooner rather than later—and it could be assessed as low, medium, or high (see Table A.2). This assessment is largely based on the risk assessment methodology originally described by Mosca, which incorporates assessments of how long information must stay secure, how long it will take to migrate to PQC, and when capable quantum computers are likely to arrive (Mosca, 2018). Essentially, if NCF operations require the communication of data with a long confidentiality lifetime (i.e., greater than ten years), the urgency for that NCF is assessed as high because that sensitive information is increasingly at risk of being captured for later exploitation until communications migrate to PQC. The longer the migration is delayed, the more the risk grows, and the urgency of swift action is high. In contrast, if an NCF is affected by remote authentication vulnerabilities that must be addressed only before a CRQC arrives and the vulnerability does not affect any long-lived hardware that might be hard to update (e.g., long-lived operational ICS technology), we assessed the NCF as low urgency. If an NCF communicates data with a moderate confidentiality lifetime (i.e., greater than one year but less than ten years), we might have assessed it as medium urgency. A similar assessment of medium urgency would be given if the NCF is affected primarily by remote authentication vulnerabilities but some factors indicate that those vulnerabilities would still be present when a CRQC arrives (e.g., in long-lived hardware that was hard to update after production).

Dependencies Among National Critical Functions

A full assessment of the dependencies among NCFs would be a significant undertaking that is outside the scope of this report. Nevertheless, urgency assessments must necessarily incorporate factors related to the dependencies among the NCFs. Many NCFs will be dependent on organizations in other NCFs to provide the solutions needed to mitigate vulnerabilities. For many NCFs, the assessment of urgency assumes that certain IT products and services supplied by other NCFs will be quickly updated and available where appropriate, and the urgency assessment for the NCF in question is an assessment of the NCF's ability to acquire and implement those products and services. The urgency for the *implementing* NCF might be low, even if the urgency for the *providing* NCF might be high.

For example, consider the case that NCF A has an authentication vulnerability in all of its operational hardware (which is produced by NCF B), and that hardware needs to be replaced with new hardware that can handle the requirements of PQC. If NCF B rapidly develops and produces new versions of the hardware that handle PQC, NCF A will make the necessary hardware updates through routine hardware obsolescence and replacement cycles well before a CRQC exists. In this case, the urgency for NCF A (the *implementer*) would be *low*, while the urgency for NCF B (the *provider*) would be *high*. Except where documentation indicates that an NCF historically does *not* keep to routine technology refresh cycles for certain relevant hardware, we assumed that many PQC migration issues would be addressed sufficiently swiftly by default through these cycles and software patches for *implementing* NCFs.

TABLE A.2
Ratings for Urgency

Rating	Definition
Low	We identified no catch-and-exploit vulnerabilities, and we anticipate no significant challenges in updating long-lived hardware.
Medium	The NCF exhibits catch-and-exploit vulnerabilities for data with a medium confidentiality lifetime (i.e., one to ten years), or the NCF might find it challenging to address authentication vulnerabilities before a CRQC arrives.
High	The NCF exhibits catch-and-exploit vulnerabilities for data with a long confidentiality lifetime (i.e., greater than ten years), or the NCF will find it very challenging to address authentication vulnerabilities before a CRQC arrives.

Even if a high urgency means that risk is growing now for catch-and-exploit vulnerabilities, any risk will only be actualized (i.e., the impact occurs) in the future when a CRQC is built. In the analysis, we assumed that such a system would be available in the mid-2030s, in line with previous estimates (Vermeer and Peet, 2020), but there is a high degree of uncertainty in this assumption. This event could arrive substantially sooner or later than this time frame. Finally, assessments of urgency assume that a vulnerability's most devastating impact *would* occur if it *could* occur. Essentially, it assumes Murphy's Law: If anything can go wrong, it will.

For example, if a widespread catch-and-exploit issue is present for an NCF, we assumed for the urgency assessment that sensitive data would be captured and later exploited. If that would lead to an impact that would disrupt the function, it would contribute to an assessment of higher urgency. Realistically, many other factors could make this unlikely or blunt the impact to a degree. Those factors are discussed in the "other factors" sections and can mitigate or exacerbate the contribution of urgency to the final assessment of priority for assistance.

Rate the Scope of the Organizations and Systems Requiring Updates

The rating on scope assesses the breadth or scale of the organizations and systems that require updates, and it could be assessed as low, medium, or high. *Scope* refers to an assessment of the approximate number of separate organizations within an NCF that require active intervention to migrate to PQC. Migration steps that are likely to happen by default (e.g., when new hardware acquired during a routine hardware refresh is designed to meet the requirements of PQC) or with little active intervention (e.g., installing available software patches) do not contribute to scope. Scope is largely confined to an approximation of the number of organizations that must take action, not the number of separate migration instances requiring attention. An assessment of high scope could, for example, be derived from an assessment that each of thousands of organizations must make a single nontrivial software update, but an assessment that a few organizations must make changes in hundreds of high-priority applications they manage would likely be classified as low scope. Although the level of effort in these two cases might be similar, the impact of intraorganizational scope on priority for assistance is largely addressed with the next metric, cost per organization, which we describe in the next section.

The ratings for scope are separated using the boundaries in Table A.3.

Approximating the scope using these boundaries allows an assessment that fits the high-level approach of our research effort. Assessing scope at this high level alongside the cost per organization (in the next rating) allows a qualitative assessment of the level of effort each NCF would require to address vulnerabilities. In other words, combining an approximation of the number of organizations in an NCF that would need to act with an approximation of the resources those required actions would entail leads to a broad assessment of level of effort needed across an NCF. This makes these important factors in our assessment of priority for assistance.

TABLE A.3
Ratings for Scope

Rating	Definition
Low	Less than ten organizations must act.
Medium	Between ten and 100 organizations must act.
High	More than 100 organizations must act.

This often practically results in assessments of how centralized the risk mitigation will be across an NCF, separating scope assessments into rough-order-of-magnitude, qualitative scenarios that can inform the desired metric: priority for assistance. Those scenarios resemble the following:

- **low:** Just a few organizations are responsible for mitigating vulnerability in a small number of shared resources. These resources could be national-level databases, standard communication protocols used to perform the function, or other networked systems that are administered by single organizations and used by many others in the NCF.
- **medium:** Vulnerabilities are still primarily in resources administered by single organizations and used by many others, but the organizations managing those resources are more numerous and less centralized. Rather than just a few national databases, the NCF might rely on many regional (e.g., state-based) networks, information-sharing systems, or databases. No vulnerabilities are present that would require unique, individual action from each organization in the NCF.
- **high:** Vulnerabilities exist that require individual action from a significant proportion of the organizations included in the NCF.

In NCFs in which most stakeholders rely on somewhat centralized guidance, regulation, or standards, just a few entities will need to take specific actions that will facilitate migration for the rest of the NCF stakeholders. In less centralized, more-diffuse NCFs, however, many stakeholders might need to invest significant resources in addressing the issues individually. The scope assessment does not explicitly assess how diffuse or centralized an NCF is, but factors identified in the "other factors" sections often provide such supplementary information.

Like in most cases, a precise accounting of the number of affected organizations in an NCF is outside the scope of these assessments. Instead, the assessments rely on a rough approximation of which of the above scenarios best describes the NCF based on analysis of open literature, industry data, and evaluations of whether systems in affected organizations require active intervention.

Rate the Relative Cost per Organization Required to Address the Vulnerabilities

We next assessed a relative cost *per organization* that will be required for an NCF to address quantum computing vulnerabilities. Cost could be rated as low, medium, or high. These ratings are assigned according to the general criteria shown in Table A.4.

TABLE A.4
Ratings for Cost

Rating	Criteria
Low	Organizations must take only limited software updates and configuration changes using known or standard tools, protocols, and guidance. Any required hardware updates can likely take place during routine hardware refreshes.
Medium	Organizations must take actions that are costlier than limited, simple software updates or configuration changes. They might need to perform limited development of custom software or perform rare off-cycle hardware replacements using commercially available hardware.
High	Organizations must take costlier actions than those just described in the medium category. These could include extensive software or protocol research, development, and testing. They could also include extensive off-cycle hardware replacement or the urgent development of novel hardware that can accommodate the requirements of PQC.

The qualitative categorization of costs in this way is informed by the context and demonstration scenarios for PQC migration recently described by NIST:

> There is currently no inventory that can guide updates to standards, guidelines, regulations, hardware, firmware, operating systems, communication protocols, cryptographic libraries, and applications that employ cryptography that meets the need to accelerate migration to quantum-resistant cryptography. (Barker, Souppaya, and Newhouse, 2021, p. 3)

NIST's effort aims to provide "a starting point for expeditiously discovering where updates to quantum-resistant cryptography will be required" (Barker, Souppaya, and Newhouse, 2021, p. 3). Because such a detailed accounting of the actions that any given NCF or organization must take does not yet exist, this analysis took the described high-level approach to assessing costs according to general categories of remediation actions, such as software updates and hardware refreshes.

Assumptions Used in Assessing Costs

When assessing costs according to these categories, we typically made several assumptions:

- First, when NCFs are dependent on other NCFs for the products and services needed to migrate systems to PQC, it is assumed that the *providing* NCFs will be able to offer those products and services in as timely a manner as is needed. This would mean, for example, that, in most cases, the novel hardware or software updates would be available for an *implementing* NCF to incorporate using extant hardware refresh cycles and software patch processes rather than rushing to adopt when the existence of a CRQC seems imminent.
- Second, it is assumed that existing hardware will be adequate to meet the requirements for post-quantum key exchange needed to mitigate catch-and-exploit vulnerabilities for *implementing* NCFs (although *providing* NCFs might have exceptions). In other words, mitigating catch-and-exploit vulnerabilities will require updates to address such issues as which standard protocols, cryptographic libraries, and configurations are used but will not require out-of-cycle hardware replacements. This assumption is based on multiple proactive efforts to evaluate this issue, test impacts of hybrid cryptography schemes, promote cryptographic algorithm agility in embedded hardware, and develop quantum-resistant hardware. Amazon Web Services, for example, has stated that post-quantum TLS is now supported (Hopkins, 2019) and has showed minimal impact on latency when testing some hybrid (i.e., combined conventional and post-quantum) TLS key exchange algorithms (Weibel, 2020). TCG has also issued guidance for secure update of software and firmware in embedded systems, with cryptographic agility needed for the PQC transition in mind (TCG, 2020). Such organizations as FutureTPM are also involved in ongoing research and collaboration on embedded hardware, such as trusted platform modules, that can support PQC (FutureTPM, undated; Truskaller, 2020).
- Finally, it is not known to what extent the migration to PQC will require widespread hardware replacements, and the discovery and evaluation of this issue are the first demonstration scenario described by the ongoing NIST PQC migration project (Barker, Souppaya, and Newhouse, 2021). Cost assessments related to hardware, therefore, generally pertain to any somewhat unique hardware used by an NCF and assume commonplace hardware (e.g., laptop computers or commercial Wi-Fi routers) will not require out-of-cycle replacement.

Identify Other Factors That Could Make the Challenges More or Less Difficult to Address

We next assessed the various other factors associated with the NCF that could make any challenges more or less difficult to address, and the possible ratings are mitigating, neutral, and exacerbating, as shown in Table A.5.

This category is less generalizable than the others because the factors that could affect an NCF's ability to address any challenges are often somewhat unique to each NCF. The factors that are identified are often those that have an impact on the previous three categories in some way; they could be factors that mitigate or exacerbate the assessed urgency, scope, or cost.

For example, if an NCF is assessed to have a high scope (meaning that it affects more than 100 organizations), the challenge might be mitigated by the presence of strong, effective industry and trade groups or supporting federal agencies that would be useful in disseminating resources and guidance to affected organizations in the NCF.

In contrast, an NCF might be rated as low urgency but have exacerbating factors in the form of documentation that suggests that the NCF has historically struggled with timely replacement of vulnerable legacy equipment and systems, suggesting that timely migration to PQC could therefore be challenging nevertheless.

A neutral rating could be assigned either when no significant other factor is present or when there is an overall balance of mitigating and exacerbating factors.

Any of a wide variety of unique factors could potentially affect an NCF's ability to address any relevant issues, but the following are some examples:

- notable availability or absence of needed human capital to support the migration
- historically proactive or behind schedule in managing IT transformation
- indications that preparations for the migration are already underway
- presence of effective professional organizations that can support the NCF via dissemination of guidance, standards, and resources
- factors that would make some organizational data in the NCF of more or less value to potential attackers
- availability of actions (not associated with PQC) that could effectively mitigate urgent vulnerability, allowing robust PQC migration to happen over a longer timescale (e.g., organizations could simply rotate keys more frequently).

Consideration of Dependencies Among National Critical Functions

In addition to these factors, we considered some of the dependencies among NCFs, especially for those NCFs that are the primary providers of the products and services needed to create a quantum-resistant information and communication infrastructure. Each of the NCFs is, by definition, *critical*, and disruption of any of the functions would have cascading effects on many others. But some NCFs will be primarily depended on to move quickly and effectively to provide quantum-resistant products and services to other dependent NCFs, and, in some cases, this will be noted as an exacerbating factor. The failure of such an NCF to make

TABLE A.5
Ratings for Other Factors

Rating	Criteria
Mitigating	Some factors could mitigate the assessed urgency, scope, or cost of addressing the quantum computing challenge for the NCF.
Neutral	Either no significant other factor is present or there is an overall balance of mitigating and exacerbating factors.
Exacerbating	Some factors could exacerbate the assessed urgency, scope, or cost of addressing the quantum computing challenge for the NCF.

the products for PQC migration available to others in a timely manner would have cascading impacts on the urgency and costs for other NCFs as they were forced to manage unaddressed vulnerabilities, find specialized solutions, and plan for costly, out-of-cycle updates when they became available.

Resilience, Degradation and Disruption, and Risk

Finally, the categories described so far have been based on *vulnerabilities* in the NCFs, not necessarily on *risk* or *resilience*. Practically, other factors associated with the NCF could indicate that it would be resilient to single, or even many, points of failure stemming from quantum computing vulnerabilities. Furthermore, some factors might suggest that many of the existing vulnerabilities would be unlikely to be exploited or that many of those vulnerabilities would be unlikely to result in significant negative impacts if they were exploited. Although a more robust treatment of the concepts of NCF resilience, degradation versus disruption, and risk assessment based on threat actors' motivations was outside the scope of this analysis, these factors might occasionally be described in this section of the assessments where they are relevant and publicly documented.

Rank the National Critical Function's Priority for Assistance

Using the ratings in the previous categories, we rated each NCF's priority for assistance as low, medium, or high. We used these ratings to categorize the NCFs according to which would benefit most from assistance from organizations across the U.S. government. Each rating is therefore meant to incorporate assessments of both where the need for assistance might be high and where the capability and resources available to the NCF might be low. As a result, it is created by assigning values to the assessments of urgency, scope, and cost and modifying those values according to the other identified mitigating or exacerbating factors.

We assigned numeric values from 1 to 3 (corresponding to low, medium, and high) to the ratings in the categories of urgency, scope, and cost. Other factors affecting those categories have the potential to modify those values by adding or subtracting a value based on the assessed impact of that factor. We then summed the modified values for the three categories to get a final numeric value that we used to assign a rating of low, medium, or high priority for assistance.

Although the assignment of numeric values to the original ratings in the three categories was straightforward, the modification of those values by the other factors is subjective and based on our judgment of the impact of those factors. An exacerbating factor might be assigned a modifying value of +1 for urgency, for example, if we deemed it to have a significant exacerbating impact on urgency, or we might have assigned a value of –0.5 to scope if we deemed that the factor had a smaller mitigating impact on scope. We based assignments of numerical boundaries between ratings for low, medium, and high priority for assistance on author judgment and applied those boundaries consistently for each NCF assessment.

Abbreviations

CISA	Cybersecurity and Infrastructure Agency
CRQC	cryptographically relevant quantum computer
DHS	U.S. Department of Homeland Security
HSOAC	Homeland Security Operational Analysis Center
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IP	intellectual property
IPsec	Internet protocol security
IT	information technology
NAICS	North American Industry Classification System
NCF	national critical function
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NSA/CSS	National Security Agency/Central Security Service
PHI	protected health information
PII	personally identifiable information
PKI	public-key infrastructure
PQC	post-quantum cryptography
R&D	research and development
S/MIME	Secure/Multipurpose Internet Mail Extensions
TCG	Trusted Computing Group
TLS	transport-layer security
VPN	virtual private network

Bibliography

Works Cited

3GPP—*See* 3rd Generation Partnership Project.

3rd Generation Partnership Project, *3GPP TS 33.105 version 15.1.0 | 5G; Security Architecture and Procedures for 5G System*, June 21, 2018.

Adler, Ericka L., "Practices Must Comply with New Medical Record Transfer Rules," *Physicians Practice*, February 21, 2013. As of October 6, 2021:
https://www.physicianspractice.com/view/practices-must-comply-new-medical-record-transfer-rules

American Public Transportation Association, *Cybersecurity Considerations for Public Transit*, recommended practice, APTA SS-ECS-RP-001-14, October 17, 2014. As of October 5, 2021:
https://www.apta.com/research-technical-resources/standards/security/apta-ss-ecs-rp-001-14/

Anderson, Ben, Sandia National Laboratories, *Securing Vehicle Charging Infrastructure: 2021 DOE Vehicle Technologies Office Annual Merit Review*, presentation at the 2021 U.S. Department of Energy Vehicle Technologies Office annual merit review on electrification, June 23, 2021. As of October 8, 2021:
https://www.energy.gov/eere/vehicles/articles/securing-vehicle-charging-infrastructure

Aon, "Cyber Vulnerability in the Construction Sector," webpage, undated. As of October 12, 2021:
https://www.aon.com/cyber-solutions/thinking/cyber-vulnerability-in-the-construction-sector/

"Apple, Google, Microsoft, and Mozilla Come Together to End TLS 1.0," Ars Technica, October 16, 2018. As of April 3, 2022:
https://arstechnica.com/gadgets/2018/10/browser-vendors-unite-to-end-support-for-20-year-old-tls-1-0/

Association of American Railroads, "Railroads and Cybersecurity," fact sheet, August 2021. As of October 1, 2021:
https://www.aar.org/wp-content/uploads/2020/09/AAR-Cybersecurity-Fact-Sheet.pdf

ATM Marketplace, "Skip to Windows 10 for Next ATM OS Migration, ATMIA Recommends," June 1, 2015. As of October 13, 2021:
https://www.atmmarketplace.com/news/skip-to-windows-10-for-next-atm-os-migration-atmia-recommends/

Austin, David, and Tamara Hayford, *Research and Development in the Pharmaceutical Industry*, Washington, D.C.: Congressional Budget Office, April 8, 2021. As of September 24, 2021:
https://www.cbo.gov/publication/57025

Baker, James, Patricia Cordeiro, Tom Doepke, Shamina Hossain-McKenzie, Christopher Howerter, Nicholas Jacobs, Deepu Jose, Christine Lai, and Jeffery Zhao, *General Requirements for Designing and Implementing a Cryptography Module for Distributed Energy Resource (DER) Systems*, Albuquerque: Sandia National Laboratories, SAND2018-9407R, June 2018. As of October 12, 2021:
https://www.osti.gov/servlets/purl/1467978

Barker, William, William Polk, and Murugiah Souppaya, "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms," white paper, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, April 28, 2021. As of September 7, 2021:
https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final

Barker, William, Murugiah Souppaya, and William Newhouse, "Migration to Post-Quantum Cryptography," project description, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, August 2021. As of October 20, 2021:
https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography

Ben Mahmoud, Mohamed Slim, Alain Pirovano, and Nicolas Larrieu, "Aeronautical Communication Transition from Analog to Digital Data: A Network Security Survey," *Computer Science Review*, Vol. 11–12, May 2014, pp. 1–29.

Best, Jo, "Could Implanted Medical Devices Be Hacked?" *BMJ*, Vol. 368, 2020, art. m102.

Better Identity Coalition, *Better Identity in America: A Blueprint for Policymakers*, July 2018. As of October 9, 2021:
https://www.betteridentity.org/

Bindel, Nina, University of Waterloo; Sarah McCarthy, Institute for Quantum Computing; Hanif Rahbari, and Geoff Twardokus, Rochester Institute of Technology, *Suitability of 3rd Round Signature Candidates for Vehicle-to-Vehicle Communication*, presentation at the Third Postquantum Cryptography Standardization Conference, June 8, 2021. As of October 5, 2021:
https://csrc.nist.gov/Presentations/2021/suitability-of-3rd-round-signature-candidates-for

Bissell, Kelly, Ryan M. LaSalle, and Paolo Dal Cin, *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study*, Accenture, March 6, 2019. As of October 14, 2021:
https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Board of Governors of the Federal Reserve System, "Designated Financial Market Utilities," webpage, last updated January 29, 2015. As of October 8, 2021:
https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm

———, "Automated Clearinghouse Services," webpage, last updated September 28, 2020. As of October 8, 2021:
https://www.federalreserve.gov/paymentsystems/fedach_about.htm

———, "Fedwire Funds Services," webpage, last updated May 7, 2021. As of October 8, 2021:
https://www.federalreserve.gov/paymentsystems/fedfunds_about.htm

Bour, Guillaume, Karin Bernsmed, Ravishankar Borgaonkar, and Per Håkon Meland, "On the Certificate Revocation Problem in the Maritime Sector," in Mikael Asplund and Simin Nadjm-Tehrani, eds., *Secure IT Systems*, proceedings of the 25th Nordic Conference on Secure Information Technology Systems, November 23–24, 2020, c. 2020, pp. 142–157. As of October 5, 2021:
https://doi.org/10.1007/978-3-030-70852-8_9

Brecht, Benedikt, "SCMS CV Pilots Documentation," webpage, Vehicle Safety Communications 5 Consortium, Crash Avoidance Metrics Partners, webpage, last modified February 20, 2018. As of April 5, 2022:
https://wiki.campllc.org/display/SCP

Byrne, Declan, "AeroMACS at a Glance: Moving Towards the Airport 3.0," Worldwide Interoperability for Microwave Access Forum, 2018.

CableLabs, "Securing Networks in the Broadband Age," *Informed Insights*, Spring 2017. As of September 21, 2021:
https://www.cablelabs.com/insights/securing-networks-broadband-age

Campagna, Matt, and Eric Crockett, Amazon Web Services, "Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)," briefing slides, Internet Engineering Task Force, September 2, 2021. As of September 15, 2021:
https://datatracker.ietf.org/doc/html/draft-campagna-tls-bike-sike-hybrid

Cao, Huan, Lili Wu, Yue Chen, Yongtao Su, Zhengchao Lei, and Chunping Zhao, "Analysis on the Security of Satellite Internet," in Wei Lu, Qiaoyan Wen, Yuqing Zhang, Bo Lang, Weiping Wen, Hanbing Yan, Chao Li, Li Ding, Ruiguang Li, and Yu Zhou, eds., *Cyber Security*, proceedings of the 17th China Cyber Security Annual Conference, August 12, 2020, pp. 193–205. As of September 27, 2021:
https://link.springer.com/chapter/10.1007/978-981-33-4922-3_14

Castellanos, Sara, "Visa, JPMorgan Are Already Preparing for Potential Quantum Cyberattacks," *Wall Street Journal*, October 9, 2020. As of October 15, 2021:
https://www.wsj.com/articles/
visa-jpmorgan-are-already-preparing-for-potential-quantum-cyberattacks-11602255213

CDC—*See* Centers for Disease Control and Prevention.

Centers for Disease Control and Prevention, "Standards to Facilitate Data Sharing," webpage, last reviewed March 5, 2014. As of October 11, 2021:
https://www.cdc.gov/nchhstp/programintegration/sc-standards.htm

———, "How Does ELR Work?" webpage, last reviewed April 6, 2021. As of October 12, 2021:
https://www.cdc.gov/elr/how-does-elr-work.html

Centers for Medicare and Medicaid Services, "Security Standards: Technical Safeguards," *HIPAA Security Series*, Vol. 2, Paper 4, May 2005, revised March 2007. As of September 28, 2021:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Chandramouli, Ramaswamy, *A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card–Based Identity Verification*, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, NISTIR 7849, March 2014. As of October 5, 2021:
https://csrc.nist.gov/publications/detail/nistir/7849/final

Chromium Projects, "CECPQ2," webpage, undated. As of September 17, 2021:
https://sites.google.com/a/chromium.org/dev/cecpq2

Cimpanu, Catalin, "Google Pauses Quantum Security Feature in Chrome Because of Buggy Middleware," *The Record*, September 1, 2021. As of September 15, 2021:
https://therecord.media/google-pauses-quantum-security-feature-in-chrome-because-of-buggy-middleware/

CISA—*See* Cybersecurity and Infrastructure Security Agency.

CISA, National Security Agency, and Office of the Director of National Intelligence—*See* Cybersecurity and Infrastructure Security Agency, National Security Agency, and Office of the Director of National Intelligence.

Clearing House, "CHIPS," webpage, undated. As of October 8, 2021:
https://www.theclearinghouse.org/payment-systems/chips

Cleveland, Frances, and Annabelle Lee, *Cyber Security for DER Systems*, version 1.0, Electric Power Research Institute, July 2013. As of October 13, 2021:
https://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf

Close, David, "How to Improve ATM Security with Remote Key Loading," blog post, ATM Marketplace, September 12, 2019. As of October 15, 2021:
https://www.atmmarketplace.com/blogs/how-to-improve-atm-security-with-remote-key-loading/

Cloudflare, "What Is the OSI Model?" webpage, undated b. As of August 24, 2021:
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

Code of Federal Regulations, Title 18, Conservation of Power and Water Resources; Chapter I, Federal Energy Regulatory Commission, Department of Energy; Subchapter B, Regulations Under the Federal Power Act; Part 37, Open Access Same-Time Information Systems. As of October 7, 2021:
https://www.ecfr.gov/current/title-18/chapter-I/subchapter-B/part-37

———, Title 18, Conservation of Power and Water Resources; Chapter I, Federal Energy Regulatory Commission, Department of Energy; Subchapter B, Regulations Under the Federal Power Act; Part 38, Standards for Public Utility Business Operations and Communications. As of October 7, 2021:
https://www.ecfr.gov/current/title-18/chapter-I/subchapter-B/part-38

———, Title 45, Public Welfare; Subtitle A, Department of Health and Human Services; Subchapter C, Administrative Data Standards and Related Requirements; Part 164, Security and Privacy; Subpart C, Security Standards for the Protection of Electronic Protected Health Information; Section 164.312, Technical Safeguards. As of April 9, 2022:
https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

Collier, Kevin, "50,000 Security Disasters Waiting to Happen: The Problem of America's Water Supplies," NBC News, June 17, 2021. As of September 7, 2021:
https://www.nbcnews.com/tech/security/
hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1, 2016. As of October 10, 2021:
https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

Committee on National Security Systems, "CNSS Policy 15: Use of Public Standards for Secure Information Sharing," October 20, 2016.

Committee on NSSs—*See* Committee on National Security Systems.

Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing; Intelligence Community Studies Board; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*, Washington, D.C.: National Academies Press, 2019.

Computer Security Resource Center, National Institute of Standards and Technology, U.S. Department of Commerce, "Post-Quantum Cryptography," webpage, January 3, 2017, last updated June 14, 2021a. As of October 9, 2021:
https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

———, "Post-Quantum Cryptography," webpage, June 14, 2021b. As of September 7, 2021:
https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Crane, Casey, "What Is a Quantum-Safe Hybrid Digital Certificate?" *Infosec Insights*, December 8, 2020. As of September 15, 2021:
https://sectigostore.com/blog/what-is-a-quantum-safe-hybrid-digital-certificate/

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, "Understanding Vulnerabilities of Positioning, Navigation, and Timing," fact sheet, undated d. As of September 23, 2021:
https://www.cisa.gov/publication/pnt-vulnerabilities-fact-sheet

———, "Public Safety Communications Evolution," January 2019a. As of October 11, 2021:
https://www.cisa.gov/sites/default/files/publications/
Public_Safety_Communications_Evolution_FINAL_01222019_508C.pdf

———, "Time: The Invisible Utility," fact sheet, March 12, 2019b. As of September 23, 2021:
https://us-cert.cisa.gov/sites/default/files/documents/
Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

———, *Emergency Services Sector Landscape*, August 2019c. As of October 8, 2021:
https://www.cisa.gov/publication/emergency-services-sector-landscape

———, *Functional Decomposition Technical Report*, February 15, 2020a.

———, "National Critical Functions: Status Update to the Critical Infrastructure Community," July 2020b. As of April 4, 2022:
https://www.cisa.gov/national-critical-functions

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security; National Security Agency; and Office of the Director of National Intelligence, "Potential Threat Vectors to 5G Infrastructure," 2021. As of April 4, 2022:
https://www.cisa.gov/5g-library

Davis, James, *Cybersecurity for Manufacturers: Securing the Digitized and Connected Factory*, MForesight, MF-TR-2017-0202, September 2017. As of October 8, 2021:
http://mforesight.org/projects-events/cyber-security-for-manufacturers/

Defense Security Service, U.S. Department of Defense, *Administration Strategy of Mitigating the Theft of U.S. Trade Secrets*, February 2013. As of September 24, 2021:
https://obamawhitehouse.archives.gov/blog/2013/02/20/
launch-administration-s-strategy-mitigate-theft-us-trade-secrets

Deodoro, Jose, Michael Gorbanyov, Majid Malaika, and Tahsin Saadi Sedik, *Quantum Computing and the Financial System: Spooky Action at a Distance?* Washington, D.C.: International Monetary Fund, Working Paper WP/21/71, March 12, 2021. As of October 14, 2021:
https://www.imf.org/en/Publications/WP/Issues/2021/03/12/
Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159

DHS—*See* U.S. Department of Homeland Security.

DHS and EPA—*See* U.S. Department of Homeland Security and U.S. Environmental Protection Agency.

DHS and U.S. Environmental Protection Agency—*See* U.S. Department of Homeland Security and U.S. Environmental Protection Agency.

Dixon, Herbert B., Jr., "Cyberattacks on Courts and Other Government Institutions," *Judges' Journal*, January 17, 2019. As of August 11, 2021:
https://www.americanbar.org/groups/judicial/publications/judges_journal/2018/summer/cyberattacks-courts-and-other-government-institutions/

Dodd–Frank Wall Street Reform and Consumer Protection Act—*See* Public Law 111-203.

Downey, Andrea, "Encryption Standards for Medical Devices 'Need to Be Mandatory,'" *Digital Health*, July 31, 2019. As of September 29, 2021:
https://www.digitalhealth.net/2019/07/encryption-standards-medical-devices-mandatory/

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee, *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, New York: Federal Reserve Bank of New York, Staff Report 909, January 2020, revised May 2021. As of October 14, 2021:
https://www.newyorkfed.org/research/staff_reports/sr909.html

Entrust, "Post Quantum Cryptography," webpage, undated. As of October 11, 2021:
https://www.entrust.com/resources/certificate-solutions/learn/post-quantum-cryptography

Executive Order 13526—*See* Obama, 2009.

FactSet, financial data and analytics, 2021. As of April 22, 2022:
http://www.factset.com

Federal Aviation Administration, U.S. Department of Transportation, *NextGen Annual Report: A Report on the History, Current Status, and Future of National Airspace System Modernization—Fiscal Year 2020*, c. 2020a. As of October 4, 2021:
https://www.faa.gov/nextgen/

———, *NAS Enterprise Architecture: Infrastructure Roadmaps v14.0—Baseline*, January 2020b. As of October 4, 2020:
https://www.faa.gov/nextgen/media/NAS_Infrastructure_Roadmaps_v14.pdf

Federal Financial Institutions Examination Council, *FFIEC Information Technology Examination Handbook*, September 2016. As of October 14, 2021:
https://ithandbook.ffiec.gov/

———, "Authentication and Access to Financial Institution Services and Systems," August 2021. As of October 8, 2021:
https://www.ffiec.gov/press/pr081121.htm

Federal Reserve Banks, "Fedwire® Funds Service: Annual Statistics," webpage, undated. As of October 8, 2021:
https://www.frbservices.org/resources/financial-services/wires/volume-value-stats/annual-stats.html

Federal Trade Commission, "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach," press release, July 22, 2019. As of October 13, 2021:
https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

Fedorov, Aleksey K., Evgeniy O. Kiktenko, and Alexander I. Lvovsky, "Quantum Computers Put Blockchain Security at Risk," *Nature*, Vol. 563, November 22, 2018, pp. 465–467.

FFIEC—*See* Federal Financial Institutions Examination Council.

Financial Industry Regulatory Authority, *2021 FINRA Industry Snapshot*, c. 2021. As of October 14, 2021:
https://www.finra.org/rules-guidance/guidance/reports-studies/2021-industry-snapshot

FINRA—*See* Financial Industry Regulatory Authority.

First Responders Group, Science and Technology Directorate, U.S. Department of Homeland Security, "Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations," January 6, 2015. As of September 23, 2021:
https://www.dhs.gov/publication/best-practices-improved-robustness-time-and-frequency-sources-fixed-locations

Fitzgerald, Caitriona, Pamela Smith, and Susannah Goodman, *The Secret Ballot at Risk: Recommendations for Protecting Democracy*, Electronic Privacy Information Center, Verified Voting Foundation, and Common Cause Education Fund, August 18, 2016. As of October 1, 2021:
https://secretballotatrisk.org/

Forum on Cyber Resilience; Cyber Resilience Workshop Series Committee; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine, *Cryptographic Agility and Interoperability: Proceedings of a Workshop*, Washington, D.C.: National Academies Press, 2017.

FutureTPM, "1st FutureTPM Workshop on Quantum-Resistant Crypto Algorithms," webpage, undated. As of August 27, 2021:
https://futuretpm.eu/events/workshops/1-st-futuretpm-workshop

Germano, Judith H., *Cybersecurity Risk and Responsibility in the Water Sector*, Denver, Colo.: American Water Works Association, 2019. As of October 13, 2021:
https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf

Google Cloud, "HL7v2," *Cloud Healthcare API*, October 5, 2021. As of October 12, 2021:
https://cloud.google.com/healthcare/docs/concepts/hl7v2

Grassi, Paul A., Michael E. Garcia, and James L. Fenton, *Digital Identity Guidelines*, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-63-3, June 2017. As of October 10, 2021:
https://doi.org/10.6028/NIST.SP.800-63-3

Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018. As of September 7, 2021:
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greene, Tim, "What Is the Internet Backbone and How It Works," *Network World*, March 12, 2020. As of October 4, 2021:
https://www.networkworld.com/article/3532318/what-is-the-internet-backbone-and-how-it-works.html

Griffor, Edward R., Christopher Greer, David A. Wollman, and Martin J. Burns, *Framework for Cyber-Physical Systems*, Vol. 1: *Overview*, version 1.0, Cyber-Physical Systems Public Working Group, Smart Grid and Cyber-Physical Systems Program Office, Engineering Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 1500-201, June 26, 2017. As of April 21, 2022:
https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview

Hall, Chris, Richard Clayton, Ross Anderson, and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem*, European Network and Information Security Agency, April 2011. As of August 16, 2021:
https://www.internetsociety.org/resources/deploy360/2012/
enisa-report-resilience-of-the-internet-interconnection-ecosystem/

Hamilton, Janet J., and Richard S. Hopkins, "Using Technologies for Data Collection and Management," in Sonja A. Rasmussen and Richard A. Goodman, eds., *The CDC Field Epidemiology Manual*, 4th ed., New York: Oxford University Press, 2019. As of October 11, 2021:
https://www.cdc.gov/eis/field-epi-manual/chapters/data-collection-management.html

Hasan, Monowar, Sibin Mohan, Takayuki Shimizu, and Hongsheng Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles*, Vol. 5, No. 4, December 2020, pp. 693–713. As of October 5, 2021:
https://doi.org/10.1109/TIV.2020.2987430

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache, "The Future of Financial Stability and Cyber Risk," Washington, D.C.: Brookings Institution, October 2018. As of October 14, 2021:
https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/

Hemsley, Kevin E., and Ronald E. Fisher, *History of Industrial Control System Cyber Incidents*, Idaho Falls: Idaho National Laboratory, INL/CON-18-44411-Revision-2, December 2018. As of April 5, 2022:
https://www.osti.gov/biblio/1505628-history-industrial-control-system-cyber-incidents

Hoffman, John T., "Food and Beverage Industry Cyber Security Risk Management: Does a HACCP-Based Food Safety Culture Provide Solutions?" *Food Safety Magazine*, September 19, 2017.

Hopkins, Andrew, "Post-Quantum TLS Now Supported in AWS KMS," *AWS Security Blog*, November 4, 2019. As of August 31, 2021:
https://aws.amazon.com/blogs/security/post-quantum-tls-now-supported-in-aws-kms/

ICS-CERT—*See* Industrial Control Systems Cyber Emergency Response Team.

Industrial Control Systems Cyber Emergency Response Team, U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*, September 2016. As of October 6, 2021:
https://www.hsdl.org/?abstract&did=797585

———, "Cyber-Attack Against Ukrainian Critical Infrastructure," Alert IR-ALERT-H-16-056-01, February 25, 2016, last revised July 20, 2021. As of September 7, 2021:
https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, *Digital Signature Standard (DSS)*, Gaithersburg, Md., Federal Information Processing Standards Publication 186-5, draft, October 2019. As of October 11, 2021:
https://csrc.nist.gov/publications/detail/fips/186/5/draft

Intelligent Transportation Systems Joint Program Office, Office of the Assistant Secretary for Research and Technology, U.S. Department of Transportation, "Connected Vehicle Standards: Research Progress and Insights," webpage, undated a. As of October 5, 2021:
https://www.its.dot.gov/research_archives/connected_vehicle/connected_vehicle_standards_progress.htm

———, Office of the Assistant Secretary for Research and Technology, U.S. Department of Transportation, "Security Credential Management System (SCMS)," webpage, undated b. As of October 5, 2021:
https://www.its.dot.gov/resources/scms.htm

International Telecommunication Union, "Information Technology: Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks," Recommendation X.509, October 2019. As of October 11, 2021:
https://www.itu.int/rec/T-REC-X.509

Irei, Alissa, and Jessica Scarpati, "Differences Among WEP, WPA, WPA2 and WPA3 Wireless Security Protocols," webpage, *TechTarget*, December 2020. As of September 30, 2021:
https://www.techtarget.com/searchnetworking/feature/
Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

IT Laboratory—*See* Information Technology Laboratory.

ITS Joint Program Office—*See* Intelligent Transportation Systems Joint Program Office.

Jackson, Brian A., Michael J. D. Vermeer, Kristin J. Leuschner, Dulani Woods, John S. Hollywood, Duren Banks, Sean E. Goodison, Joe Russo, and Shoshana R. Shelton, *Fostering Innovation Across the U.S. Criminal Justice System: Identifying Opportunities to Improve Effectiveness, Efficiency, and Fairness*, Santa Monica, Calif.: RAND Corporation, RR-4242-NIJ, 2020. As of April 5, 2022:
https://www.rand.org/pubs/research_reports/RR4242.html

Kessler, Gary C., "An Overview of Cryptography," webpage, July 28, 2021. As of October 11, 2021:
https://www.garykessler.net/library/crypto.html

Koukounas, Aggelos, Eleni Vytogianni, and Marnix Dekker, *7 Steps to Shore Up BGP*, European Union Agency for Network and Information Security, May 2019. As of April 5, 2022:
https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp

Kuzlu, Murat, Manisa Pipattanasomporn, and Saifur Rahman, "Communication Network Requirements for Major Smart Grid Applications in HAN, NAN and WAN," *Computer Networks*, Vol. 67, July 4, 2014, pp. 74–88.

Kwiatkowski, Kris, and Luke Valenta, "The TLS Post-Quantum Experiment," blog post, Cloudflare, October 30, 2019. As of September 15, 2021:
https://blog.cloudflare.com/the-tls-post-quantum-experiment/

Laufman, David H., Joseph M. Casino, and Michael J. Kasdan, "The Department of Justice's National Security Division Chief Addresses China's Campaign to Steal U.S. Intellectual Property," *National Law Review*, Vol. 10, No. 237, August 24, 2020. As of October 8, 2021:
https://www.natlawreview.com/article/
department-justice-s-national-security-division-chief-addresses-china-s-campaign-to

Laughlin, Nick, and Peyton Shelburne, "How Voters' Trust in Elections Shifted in Response to Biden's Victory," *Morning Consult*, last updated January 27, 2021. As October 5, 2021:
https://morningconsult.com/form/tracking-voter-trust-in-elections/

Lexova, Ingrid, "Manufacturing Faces Distinct Challenges in Cyber Risk Mitigation," webpage, *S&P Global Commodity Insights*, January 28, 2021. As of October 8, 2021:
https://www.spglobal.com/platts/en/market-insights/latest-news/
metals/012821-feature-manufacturing-faces-distinct-challenges-in-cyber-risk-mitigation

"LIMS Vendor," *LIMSWiki*, October 6, 2021. As of October 12, 2021:
https://www.limswiki.org/index.php/LIMS_vendor

Littman, Marlyn Kemper, "Satellite Network Security," in Mehdi Khosrow-Pour, ed., *Encyclopedia of Information Science and Technology*, 2nd ed., Hershey, Pa.: Information Resources Management Association, 2009, pp. 3350–3355.

Local Control Working Group, Technology and Broadband Committee, National Public Safety Telecommunications Council, *Public Safety Entity Control and Monitoring Requirements for the Nationwide Public Safety Broadband Network*, final report, October 2015. As of October 11, 2021:
https://www.npstc.org/
download.jsp?tableId=37&column=217&id=3556&file=NPSTC_Local_Control_Report_Final_20151010.pdf

Lockwood, John W., Adwait Gupta, Nishit Mehta, Michaela Blott, Tom English, and Kees Vissers, "A Low-Latency Library in FPGA Hardware for High-Frequency Trading (HFT)," *2012 IEEE 20th Annual Symposium on High-Performance Interconnects*, 2012, pp. 9–16.

MacDonald-Evoy, Jerod, "Parts of the Election System Are Ripe for Hacking: 'Encryption? We Don't Do That,'" *Maryland Matters*, October 6, 2020. As of October 1, 2021:
https://www.marylandmatters.org/2020/10/06/
parts-of-the-election-system-are-ripe-for-hacking-encryption-we-dont-do-that/

Manulis, M., C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber Security in New Space," *International Journal of Information Security*, Vol. 20, June 2021, pp. 287–311. As of April 5, 2022:
https://link.springer.com/article/10.1007/s10207-020-00503-w

Markets and Markets, "Pipeline Transportation Market by Solution (Security Solutions, Automation and Control, Integrity and Tracking Solutions, Network Communication Solutions, and Other), by Services (Consulting Service, Managed Service, Maintenance and Support), by Type (Oil and Gas, Coal, Chemical, Water, and Other): Global Forecast to 2019," webpage, undated. As of August 24, 2021:
https://www.marketsandmarkets.com/Market-Reports/pipeline-transportation-market-110375125.html

Marston, Theodore U., "The US Electric Power System Infrastructure and Its Vulnerabilities," *The Bridge*, Vol. 48, No. 2, June 15, 2018, pp. 31–39. As of October 8, 2021:
https://www.nae.edu/183133/The-US-Electric-Power-System-Infrastructure-and-Its-Vulnerabilities

Mäurer, Nils, and Arne Bilzhause, "A Cybersecurity Architecture for the L-Band Digital Aeronautical Communications System (LDACS)," *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, 2018, pp. 1–10.

Menn, Joseph, "Microsoft Warns Thousands of Cloud Customers of Exposed Databases," Reuters, August 27, 2021. As of September 14, 2021:
https://www.reuters.com/technology/
exclusive-microsoft-warns-thousands-cloud-customers-exposed-databases-emails-2021-08-26/

Mielke, Daniel M., Nils Mäurer, Thomas Gräupl, and Miguel Bellido-Manganell, "Getting Civil Aviation Ready for the Post Quantum Age with LDACS," *Digitale Welt*, Vol. 5, 2021, pp. 28–33.

Mitchell, Chris J., "The Impact of Quantum Computing on Real-World Security: A 5G Case Study," *Computers and Security*, Vol. 93, June 2020, art. 101825.

MITRE, "ATT&CK," webpage, undated. As of August 24, 2021:
https://attack.mitre.org/

Morrison, Sara, "How a Major Oil Pipeline Got Held for Ransom," *Recode*, June 8, 2021. As of September 7, 2021:
https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

Mosca, Michele, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security and Privacy*, Vol. 16, No. 5, September–October 2018, pp. 38–41.

Mozilla, "Common CA Database," webpage, undated. As of October 11, 2021:
https://www.ccadb.org/resources

NAESB—*See* North American Energy Standards Board.

National Association of Broadcasters, *The Essential Guide to Broadcasting Cybersecurity: Background and Critical Activities Every Broadcaster Should Know*, March 2016.

National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education, homepage, undated. As of October 7, 2021:
https://nces.ed.gov/

National Conference of State Legislatures, "Electronic Transmission of Ballots," webpage, September 5, 2019b. As of October 1, 2021:
https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx

National Coordination Office for Space-Based PNT—*See* National Coordination Office for Space-Based Positioning, Navigation, and Timing.

National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Performance Standards and Specifications," webpage, last modified September 2, 2020. As of September 23, 2021:
https://www.gps.gov/technical/ps/

National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, "National Critical Functions: An Evolved Lens for Critical Infrastructure Security and Resilience," April 30, 2019. As of October 21, 2021:
https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf

National Security Agency/Central Security Service, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," webpage, undated. As of October 19, 2021:
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

———, "Commercial National Security Algorithm Suite," webpage, last reviewed August 19, 2015. As of September 28, 2021:
https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

———, "Quantum Computing and Post-Quantum Cryptography," frequently asked questions, PP-21-1120, August 2021. As of September 28, 2021:
https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Secure Government Communications*, August 20, 2013. As of October 9, 2021:
https://nsarchive.gwu.edu/sites/default/files/documents/5985931/
National-Security-Archive-Department-of-Homeland.pdf

———, *NSTAC Report to the President on a Cybersecurity Moonshot*, November 14, 2018. As of October 9, 2021:
https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf

NERC—*See* North American Electric Reliability Corporation.

NIST—*See* National Institute of Standards and Technology.

North American Industry Classification System Association, "NAICS and SIC Identification Tools," webpage, undated. As of August 16, 2021:
https://www.naics.com/search/

NRMC—*See* National Risk Management Center.

NSA/CSS—*See* National Security Agency/Central Security Service.

NSTAC—*See* National Security Telecommunications Advisory Committee.

Nygaard, M., and S. Mukhopadyay, *Dragonstone Strategy: State of Cybersecurity in the Oil and Natural Gas Sector*, Livermore, Calif.: Lawrence Livermore National Laboratory, LLNL-TR-805864, February 5, 2020. As of October 12, 2021:
https://www.osti.gov/servlets/purl/1602649

Obama, Barack, "Classified National Security Information," Washington, D.C.: White House, Executive Order 13526, December 29, 2009. As of September 30, 2021:
https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

O'Donoghue, Karen, "A New Security Mechanism for the Network Time Protocol," *IETF Journal*, October 31, 2017. As of September 23, 2021:
https://www.ietfjournal.org/a-new-security-mechanism-for-the-network-time-protocol/

Office for Civil Rights, U.S. Department of Health and Human Services, "Health Information of Deceased Individuals," webpage, last reviewed September 19, 2013. As of September 28, 2021:
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html

Office of Electricity, U.S. Department of Energy, "ADMS Research and Development," webpage, undated. As of October 13, 2021:
https://www.smartgrid.gov/adms_research_and_development/

Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, *United States Electricity Industry Primer*, DOE/OE-0017, July 2015. As of April 5, 2022:
https://www.energy.gov/indianenergy/downloads/united-states-electricity-industry-primer

Office of Science and Technology Policy, White House, *Enhancing the Security and Integrity of America's Research Enterprise*, Washington, D.C., c. July 2020. As of September 24, 2021:
https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf

Oil and Natural Gas Subsector Coordinating Council, Natural Gas Council, *Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry*, c. 2018. As of October 12, 2021:
https://www.api.org/news-policy-and-issues/cybersecurity/defense-in-depth-cybersecurity-in-the-natural-gas-and-oil-industry

ONG Subsector Coordinating Council—*See* Oil and Natural Gas Subsector Coordinating Council.

Pala, Massimiliano, "A Proposal for a Long-Term Post-Quantum Transitioning Strategy for Broadband Industry via Composite Crypto and PQPs," blog post, *Informed*, October 22, 2020. As of September 21, 2021:
https://www.cablelabs.com/a-proposal-for-a-long-term-post-quantum-transitioning-strategy-for-the-broadband-industry-via-composite-crypto-and-pqps

———, "Practical Considerations for Post-Quantum Cryptography Deployment," blog post, *Informed*, August 17, 2021. As of September 21, 2021:
https://www.cablelabs.com/practical-considerations-for-post-quantum-cryptography-deployment

Paquin, Christian, Douglas Stebila, and Goutam Tamvada, "Benchmarking Post-Quantum Cryptography in TLS," Cryptology ePrint, February 6, 2020. As of September 15, 2021:
https://eprint.iacr.org/2019/1447.pdf

Parent Coalition for Student Privacy, "State Student Privacy Laws," webpage, undated. As of October 7, 2021:
https://studentprivacymatters.org/state-legislation/

Parkinson, Edward, "FirstNet Is Interoperability," blog post, FirstNet Authority, October 29, 2020. As of October 11, 2021:
https://firstnet.gov/newsroom/blog/firstnet-interoperability

Payment Card Industry Security Standards Council, "Payment Card Industry Security Standards," October 2010. As of October 11, 2021:
https://www.pcisecuritystandards.org/documents/PCI%20SSC%20-%20Overview.pdf

Petrenko, Kyrylo, Atefeh Mashatan, and Farid Shirazi, "Assessing the Quantum-Resistant Cryptographic Agility of Routing and Switching IT Network Infrastructure in a Large-Size Financial Organization," *Journal of Information Security and Applications*, Vol. 46, June 2019, pp. 151–163.

Priority Criminal Justice Needs Initiative, homepage, undated. As of August 17, 2021:
https://www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs.html

Prodan, Marianna, "New Best Practices in Patient Data Transfer for EMTALA Support," *Health IT Outcomes*, April 13, 2018. As of October 6, 2021:
https://www.healthitoutcomes.com/doc/new-best-practices-in-patient-data-transfer-for-emtala-support-0001

Public Law 99-410, Uniformed and Overseas Citizens Absentee Voting Act, August 28, 1986. As of April 9, 2022:
https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg924.pdf

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996, August 21, 1996. As of April 9, 2022:
https://www.govinfo.gov/app/details/PLAW-104publ191

Public Law 107-296, Homeland Security Act of 2002, November 25, 2002. As of May 12, 2019:
https://www.govinfo.gov/app/details/PLAW-107publ296

Public Law 111-203, Dodd–Frank Wall Street Reform and Consumer Protection Act, July 21, 2010. As of April 10, 2022:
https://www.govinfo.gov/app/details/PLAW-111publ203

Rail Information Security Committee, Association of American Railroads, *Cyber Security Effective Practices for Information Technology Procurements*, April 2018. As of October 1, 2021:
https://www.aar.org/data/cyber-security-effective-practices-for-information-technology-procurements/

Reichard, Jeffrey, "Intellectual Property for the Construction Industry," webpage, JD Supra, January 22, 2018. As of October 12, 2021:
https://www.jdsupra.com/legalnews/intellectual-property-for-the-25448/

Reinhart, R. J., "Faith in Elections in Relatively Short Supply in U.S.," Gallup, February 13, 2020. As of October 5, 2021:
https://news.gallup.com/poll/285608/faith-elections-relatively-short-supply.aspx

Risk Lexicon—See Risk Steering Committee, 2010.

Risk Steering Committee, U.S. Department of Homeland Security, *DHS Risk Lexicon*, 2010 ed., September 2010. As of April 5, 2022:
https://www.cisa.gov/dhs-risk-lexicon

Road map—*See* U.S. Department of Homeland Security, 2021.

Salowey, Joseph A., Sean Turner, and Christopher A. Wood, "TLS 1.3: One Year Later," blog post, *IETF News*, December 17, 2019. As of October 21, 2021:
https://www.ietf.org/blog/tls13-adoption/

Satellite Industry Association, "Cybersecurity," webpage, undated. As of September 28, 2021:
https://sia.org/policy/cybersecurity/

Sawyer, Scott, "Cyberattacks to Metal Fabrication Companies Are Not Hypothetical," *The Fabricator*, September 24, 2021. As of October 8, 2021:
https://www.thefabricator.com/thefabricator/article/cadcamsoftware/cyberattacks-to-metal-fabrication-companies-are-not-hypothetical

Security Working Group, Federal Partnership for Interoperable Communications, "Considerations for Encryption in Public Safety Radio Systems," September 2016. As of September 24, 2021:
https://www.cisa.gov/sites/default/files/publications/20160830%20Considerations%20for%20Encryption_Final%20Draft508_0.pdf

Shor, Peter W., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

Smart Grid Cybersecurity Committee, Smart Grid Interoperability Panel, National Institute of Standards and Technology, U.S. Department of Commerce, *Guidelines for Smart Grid Cybersecurity*, Vol. 1: *Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, Gaithersburg, Md., NISTIR 7628, rev. 1, September 2014. As of October 8, 2021:
https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

Smith, Brian, and Amyn Moolji, *A Financial System That Creates Economic Opportunities: Capital Markets*, Washington, D.C.: U.S. Department of the Treasury, October 2017. As of April 5, 2022:
https://home.treasury.gov/system/files/136/A-Financial-System-Capital-Markets-FINAL-FINAL.pdf

Snell, Elizabeth, "Anthem Health Data Breach Could Compromise PII of 80M," *Health IT Security*, February 5, 2015a. As of September 28, 2021:
https://healthitsecurity.com/news/anthem-health-data-breach-could-compromise-pii-of-80m

———, "Premera Health Data Breach May Affect 11M," *Health IT Security*, March 17, 2015b. As of September 28, 2021:
https://healthitsecurity.com/news/premera-health-data-breach-may-affect-11m

Snoke, Timur, "Best Practices for NTP Services," blog post, Software Engineering Institute, April 3, 2017. As of September 23, 2021:
https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services/

Society for Worldwide Interbank Financial Telecommunication, "Monthly FIN Traffic Evolution," webpage, undated. As of October 8, 2021:
https://www.swift.com/about-us/discover-swift/fin-traffic-figures

———, *SWIFT Qualified Certificates for Electronic Seals: PKI Disclosure Statement*, June 11, 2021. As of October 8, 2021:
https://www.swift.com/swift-qualified-certificates

Soper, Daniel S., "Satellite Encryption," in John R. Vacca, ed., *Computer and Information Security Handbook*, Amsterdam: Elsevier, 2009, pp. 456–457.

Sporny, Manu, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen, "Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations," World Wide Web Consortium, proposed recommendation, August 3, 2021. As of October 11, 2021:
https://www.w3.org/TR/did-core/

Stebila, Douglas, and Michele Mosca, "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project," in Roberto Avanzi and Howard Heys, eds., *Selected Areas in Cryptography (SAC) 2016*, *LNCS*, Vol. 10532, October 2017, pp. 1–24. As of April 5, 2022:
https://openquantumsafe.org/research/

Stiennon, Richard, "Flame's MD5 Collision Is the Most Worrisome Security Discovery of 2021," *Forbes*, June 14, 2012. As of September 14, 2021:
https://www.forbes.com/sites/richardstiennon/2012/06/14/
flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012/

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-82, rev. 2, May 2015. As of October 6, 2021:
https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Streng, Stephen, *Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing*, Food Protection and Defense Institute, September 2019. As of October 12, 2021:
https://conservancy.umn.edu/handle/11299/217703

SWIFT—*See* Society for Worldwide Interbank Financial Telecommunication.

TCG—*See* Trusted Computing Group.

Technical Advisory Board for First Responder Interoperability, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, May 22, 2012. As of October 11, 2021:
https://ecfsapi.fcc.gov/file/7021919873.pdf

ThousandEyes, "ISP Tiers: Internet Service Provider 3-Tier Model," webpage, undated. As of October 4, 2021:
https://www.thousandeyes.com/learning/techtorials/isp-tiers

Toshiba Corporation, "Beginning Joint Verification Tests on Quantum Cryptography Technology to Enhance Cybersecurity in the Financial Sector: Testing Practicality in Large-Capacity and Low-Latency Communications in Stock Transactions," news release, December 21, 2020. As of October 15, 2021:
https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/20/2012-04.html

Truskaller, Martina, "FutureTPM Meeting with the Trusted Computing Group (TCG)," blog post, FutureTPM, July 29, 2020. As of August 27, 2021:
https://futuretpm.eu/index.php/blog/76-meetings/
212-futuretpm-meeting-with-the-trusted-computing-group-tcg

Truskovsky, Alexander, Daniel Van Geest, Scott Fluhrer, Panos Kampanakis, Mike Ounsworth, and Serge Mister, "Multiple Public-Key Algorithm X.509 Certificates," Internet Engineering Task Force, August 29, 2018. As of September 15, 2021:
https://datatracker.ietf.org/doc/html/draft-truskovsky-lamps-pq-hybrid-x509-01

Trusted Computing Group, *TCG Guidance for Secure Update of Software and Firmware on Embedded Systems*, version 1.0, rev. 72, February 10, 2020. As of August 27, 2021:
https://trustedcomputinggroup.org/resource/
tcg-guidance-for-secure-update-of-software-and-firmware-on-embedded-systems/

Union of Concerned Scientists, "UCS Satellite Database," webpage, version 5-1-2021, May 1, 2021. As of September 28, 2021:
https://www.ucsusa.org/resources/satellite-database

USA.gov, "Credit Reports and Scores," webpage, October 1, 2021. As of October 15, 2021:
https://www.usa.gov/credit-reports

U.S. Code, Title 6, Domestic Security; Chapter 1, Homeland Security Organization; Subchapter III, Science and Technology in Support of Homeland Security; Section 185, Federally Funded Research and Development Centers. As of March 20, 2021:
https://uscode.house.gov/view.xhtml?req=(title:6%20section:185%20edition:prelim)

———, Title 15, Commerce and Trade; Chapter 91, Children's Online Privacy Protection. As of April 9, 2022:
http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter91&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGUxNS1zZWN0aW9uNjUwMQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim

———, Title 20, Education; Chapter 31, General Provisions Concerning Education; Subchapter III, General Requirements and Conditions Concerning Operation and Administration of Education Programs: General Authority of Secretary; Part 4, Records; Privacy; Limitation on Withholding Federal Funds; Section 1232g, Family Educational and Privacy Rights. As of April 9, 2022:
https://uscode.house.gov/view.xhtml?req=(title:20%20section:1232g%20edition:prelim)

———, Title 44, Public Printing and Documents; Chapter 35, Coordination of Federal Information Policy; Subchapter II, Information Security; Section 3552, Definitions. As of March 3, 2022:
https://uscode.house.gov/view.xhtml?req=(title:44%20section:3552%20edition:prelim)

U.S. Department of Energy, *Electricity Subsector Cybersecurity: Risk Management Process*, DOE/OE-0003, May 2012. As of April 6, 2022:
https://www.hsdl.org/?abstract&did=752826

U.S. Department of Homeland Security, *Information Technology Sector Baseline Risk Assessment*, August 2009. As of April 5, 2022:
https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf

———, *Communications Sector–Specific Plan: An Annex to the NIPP 2013*, 2015. As of September 28, 2021:
https://www.hsdl.org/?abstract&did=796518

———, *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*, January 2017a. As of September 23, 2021:
https://www.dhs.gov/science-and-technology/pnt-program

———, "Emergency Services Sector Profile," November 2017b. As of October 8, 2021:
https://www.cisa.gov/publication/emergency-services-sector-profile

———, *Threats to Precision Agriculture*, October 3, 2018. As of October 12, 2021:
https://www.cisa.gov/uscert/ncas/current-activity/2018/10/03/Cybersecurity-Threats-Precision-Agriculture

———, "Post-Quantum Cryptography," webpage, October 5, 2021. As of October 15, 2021:
https://www.dhs.gov/quantum

U.S. Department of Homeland Security and U.S. Environmental Protection Agency, *Water and Wastewater Systems Sector–Specific Plan*, 2015. As of October 13, 2021:
https://www.cisa.gov/publication/nipp-ssp-water-2015

Van Deynse, David, "Certificates and Different PKIs in DOCSIS 3.1," *Excentis*, July 17, 2015. As of September 21, 2021:
https://www.excentis.com/blog/certificates-and-different-pkis-docsis-31

Vermeer, Michael J. D., and Evan D. Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*, Santa Monica, Calif.: RAND Corporation, RR-3102-RC, 2020. As of April 5, 2022:
https://www.rand.org/pubs/research_reports/RR3102.html

Von Zastrow, Claus, and Zeke Perez, Jr., "Using State Data Systems to Create an Information Culture in Education," Education Commission of the States, April 15, 2019. As of October 7, 2021:
https://www.ecs.org/using-state-data-systems-to-create-an-information-culture-in-education/

Voreacos, David, Katherine Chiglinsky, and Riley Griffin, "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?" *Bloomberg*, December 3, 2019.

Walters, Dan, "Finally, a School Data System Emerging," CalMatters, March 4, 2020. As of October 7, 2021:
https://calmatters.org/commentary/2020/03/school-data-system-education-student/

Warwick, W. M., T. D. Hardy, M. G. Hoffman, and J. S. Homer, *Electricity Distribution System Baseline Report*, Richland, Wash.: Pacific Northwest National Laboratory, PNNL-25178, July 2016. As of October 8, 2021:
https://www.energy.gov/sites/prod/files/2017/01/f34/
Electricity%20Distribution%20System%20Baseline%20Report.pdf

Weibel, Alex, "Round 2 Post-Quantum TLS Is Now Supported in AWS KMS," *AWS Security Blog*, November 16, 2020. As of August 31, 2021:
https://aws.amazon.com/blogs/security/round-2-post-quantum-tls-is-now-supported-in-aws-kms/

Weiner, Stacy, "The Growing Threat of Ransomware Attacks on Hospitals," Association of American Medical Colleges, July 20, 2021. As of September 7, 2021:
https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

WEQ—*See* Wholesale Electric Quadrant.

Werner, Debra, "Small Satellite Sector Grapples with Cybersecurity Requirements, Cost," *SpaceNews*, August 8, 2018. As of September 28, 2021:
https://spacenews.com/small-satellite-sector-grapples-with-cybersecurity-requirements-cost/

Wholesale Electric Quadrant, North American Energy Standards Board, *Public Key Infrastructure (PKI)*, Standard WEQ-012, version 002.1, March 11, 2009.

———, *Standards for Business Practices and Communication Protocols for Public Utilities: Report of the North American Energy Standards Board*, March 30, 2020. As of October 7, 2021:
https://www.naesb.org/pdf4/naesb_033020_weq_version_003.3_report.pdf

Witty, Jason, "With AI and Quantum Computing, Intelligence Sharing Is Imperative," webpage, *Insights*, November 2019. As of October 8, 2021:
https://www.fsisac.com/insights/ai-quantum-computing-intelligence-sharing

Wofford, Benjamin, "A Texas County Clerk's Bold Crusade to Transform How We Vote," *Wired*, September 15, 2020. As of October 1, 2021:
https://www.wired.com/story/dana-debeauvoir-texas-county-clerk-voting-tech-revolution/

Working Group 4, Communications Security, Reliability and Interoperability Council IV, *Final Report*, March 2015. As of April 4, 2022:
https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

Yang, Xing, Lei Shu, Jianing Chen, Mohamed Amine Ferrag, Jun Wu, Edmond Nurellari, and Kai Huang, "A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges," *IEEE/CAA Journal of Automatica Sinica*, Vol. 8, No. 2, February 2021, pp. 273–302.

Zardoshti, Anahita, *The Impacts of Quantum Computing on Insurance*, Lloyd's of London, February 2021.

Related Reading

Bartock, Michael, Joseph Brule, Ya-Shian Li-Baboud, Suzanne Lightman, James McCarthy, Karen Reczek, Doug Northrip, Arthur Scholz, and Theresa Suloway, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, NISTIR 8323, February 2021. As of April 3, 2022:
https://csrc.nist.gov/publications/detail/nistir/8323/final

Bindel, Nina, Udyani Herath, Matthew McKague, and Douglas Stebila, "Transitioning to a Quantum-Resistant Public-Key Infrastructure," *PQCrypto 2017*, May 24, 2017. As of September 15, 2021:
https://eprint.iacr.org/2017/460

Broadband Internet Technical Advisory Group, *Interconnection and Traffic Exchange on the Internet*, technical working group report, November 2014. As of September 21, 2021:
https://www.bitag.org/documents/Interconnection-and-Traffic-Exchange-on-the-Internet.pdf

Cloudflare, "What Is IPsec? How IPsec VPNs Work," webpage, undated a. As of September 15, 2021:
https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, "Emergency Communications," webpage, undated a. As of October 11, 2021:
https://www.cisa.gov/emergency-communications

———, "Emergency Services Sector Cybersecurity Initiative," webpage, undated b. As of October 8, 2021:
https://www.cisa.gov/publication/emergency-services-sector-cybersecurity-initiative

———, "Positioning Navigation and Timing," webpage, undated c. As of September 23, 2021:
https://www.cisa.gov/pnt

———, "Election Security Rumor vs. Reality," webpage, last updated November 2, 2021. As of April 4, 2022:
https://www.cisa.gov/rumorcontrol

Denholm, Paul, Robert Margolis, Bryan Palmintier, Clayton Barrows, Eduardo Ibanez, Lori Bird, and Jarett Zuboy, *Methods for Analyzing the Benefits and Costs of Distributed Photovoltaic Generation to the U.S. Electric Utility System*, National Renewable Energy Laboratory, Office of Energy Efficiency and Renewable Energy, U.S. Department of Energy, Technical Report NREL/TP-6A20-62447, September 2014. As of October 11, 2021:
https://www.osti.gov/biblio/1159357

Hodgson, Quentin E., Marygail K. Brauner, and Edward W. Chan, *Securing U.S. Elections Against Cyber Threats: Considerations for Supply Chain Risk Management*, Santa Monica, Calif.: RAND Corporation, PE-A512-1, 2020. As of April 5, 2022:
https://www.rand.org/pubs/perspectives/PEA512-1.html

International Civil Aviation Organization, *2016–2030 Global Air Navigation Plan*, 5th ed., Doc 9750-AN/963, 2016. As of April 5, 2022:
https://www.icao.int/publications/Pages/Publication.aspx?docnum=9750

JASON, MITRE Corporation, *Fundamental Research Security*, McLean, Va., JSR-19-2I, December 2019. As of September 24, 2021:
https://www.nsf.gov/news/news_summ.jsp?cntn_id=299700

Keyfactor, "What Is PKI and How Does It Work?" webpage, undated. As of September 15, 2021:
https://www.keyfactor.com/resources/what-is-pki/

Lak, Meoin, Anthony Johnson, Brenden Russell, and Manuel Avendaño, "Grid Management System: A Key Enabler of Grid Modernization," IEEE Smart Grid, August 2019. As of October 12, 2021:
https://smartgrid.ieee.org/newsletters/august-2019/grid-management-system-a-key-enabler-of-grid-modernization

Loshin, Peter, and Mike Chapple, "How to Encrypt and Secure a Website Using HTTPS," webpage, *TechTarget*, undated.

McCarthy, Jim, Otis Alexander, Sallie Edwards, Don Faatz, Chris Peloquin, Susan Symington, Andre Thibault, John Wiltberger, and Karen Viani, *Situational Awareness for Electric Utilities*, Gaithersburg, Md.: National Institute for Standards and Technology, U.S. Department of Commerce, NIST Special Publication 1800-7, August 2019. As of October 7, 2021:
https://csrc.nist.gov/publications/detail/sp/1800-7/final

National Conference of State Legislatures, "Election Security: State Policies," webpage, August 2, 2019a. As of October 1, 2021:
https://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx

North American Electric Reliability Corporation, "CIP Standards," webpage, undated. As of October 7, 2021:
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Open Access Technology International, "OATI Continues Cyber Security Commitment Through Successful WEQ-012 PKI Business Practice Standards Audit," webpage, April 7, 2021. As of October 7, 2021:
https://www.oati.com/Newsroom/Press-Coverage/weq-012-2020-audit

Red Hat, "What Is Middleware?" webpage, March 21, 2018. As of September 17, 2021:
https://www.redhat.com/en/topics/middleware/what-is-middleware

Sriram, Kotikalapudi, and Doug Montgomery, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, Gaithersburg, Md.: Advanced Network Technology Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-189, December 2019. As of October 4, 2021:
https://csrc.nist.gov/publications/detail/sp/800-189/final

Transformer Resilience and Advanced Components Program, Office of Electricity, U.S. Department of Energy, *Solid State Power Substation Technology Roadmap*, June 2020. As of October 11, 2021:
https://www.energy.gov/oe/downloads/solid-state-power-substation-technology-roadmap

U.S. Department of the Treasury, Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, Financial and Banking Information Infrastructure Committee, and U.S. Department of Homeland Security, *Financial Services Sector–Specific Plan*, c. 2015. As of October 15, 2021:
https://www.cisa.gov/publication/nipp-ssp-financial-services-2015

Van Beijnum, Iljitsch, "Meet DOCSIS, Part 1: The Unsung Hero of High-Speed Cable Internet Access," *Ars Technica*, May 5, 2011. As of September 21, 2021:
https://arstechnica.com/information-technology/2011/05/docsis-the-unsung-hero-of-high-speed-cable-internet-access/

Water Information Sharing and Analysis Center, *15 Cybersecurity Fundamentals for Water and Wastewater Utilities: Best Practices to Reduce Exploitable Weaknesses and Attacks*, Washington, D.C., June 3, 2019. As of October 13, 2021:
https://www.waterisac.org/fundamentals

Wholesale Electric Quadrant, North American Energy Standards Board, "Wholesale Electric Quadrant Standards and Implementation Guides," webpage, undated. As of October 7, 2021:
https://www.naesb.org/weq/weq_standards.asp

Future quantum computing capabilities are expected to be able to break the security of current implementations of public-key cryptography. Public-key cryptography forms the foundational building block of security for national information and communication infrastructure. Quantum computers will therefore create vulnerabilities in critical infrastructure, although migrating to new post-quantum cryptography standards being developed by the National Institute of Standards and Technology should mitigate vulnerabilities.

The U.S. Department of Homeland Security asked the Homeland Security Operational Analysis Center to perform high-level assessments of quantum vulnerabilities in the 55 national critical functions (NCFs) identified by the department. Researchers evaluated the significant issues affecting each NCF, then rated each NCF in the categories of urgency, scope, cost per organization, and other mitigating or exacerbating factors. The researchers then combined these ratings to create an assessment of each NCF's priority for assistance. They rated six of the NCFs as high priority for assistance, 15 as medium priority, and 34 as low priority. In addition, the team identified three NCFs as critical enablers of the transition to the new cryptographic standard. Finally, the researchers identified four key findings: (1) All NCFs need to prepare for the transition, (2) a significant portion of the vulnerability can be addressed with relatively few actions by the critical enablers, (3) catch-and-exploit vulnerabilities are urgent for only a few stakeholders, and (4) many factors related to the cryptographic transition are still uncertain and in need of more-detailed assessment.

$22.00

ISBN-10 197740966-0
ISBN-13 9781977409669

Cover image: Metamorworks/Getty Images.
RR-A1367-6