Preparing for Post-Quantum Critical Infrastructure

Assessments of Quantum Computing Vulnerabilities of National Critical Functions: Appendix

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

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED
About This Appendix

The Homeland Security Operational Analysis Center (HSAOC) 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, HSAOC was asked to perform an analysis of the vulnerabilities in national critical functions (NCFs) from future quantum computing capabilities. This appendix contains assessments of the quantum computing vulnerabilities affecting each of the 55 NCFs. These 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 HSAOC 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 70RCSA21FR000023, 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 or to read the main report, see www.rand.org/t/RRA1367-6.
## Contents

**APPENDIX B**

Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

<table>
<thead>
<tr>
<th>National Critical Function</th>
<th>NCF</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Critical Function 1, Operate Core Network</td>
<td>NCF01-1</td>
</tr>
<tr>
<td>National Critical Function 2, Provide Cable Access Network Services</td>
<td>NCF02-1</td>
</tr>
<tr>
<td>National Critical Function 3, Provide Internet Based Content, Information, and Communication Services</td>
<td>NCF03-1</td>
</tr>
<tr>
<td>National Critical Function 4, Provide Internet Routing, Access, and Connection Services</td>
<td>NCF04-1</td>
</tr>
<tr>
<td>National Critical Function 5, Provide Positioning, Navigation, and Timing Services</td>
<td>NCF05-1</td>
</tr>
<tr>
<td>National Critical Function 6, Provide Radio Broadcast Access Network Services</td>
<td>NCF06-1</td>
</tr>
<tr>
<td>National Critical Function 7, Provide Satellite Access Network Services</td>
<td>NCF07-1</td>
</tr>
<tr>
<td>National Critical Function 8, Provide Wireless Access Network Services</td>
<td>NCF08-1</td>
</tr>
<tr>
<td>National Critical Function 9, Provide Wireline Access Network Services</td>
<td>NCF09-1</td>
</tr>
<tr>
<td>National Critical Function 10, Distribute Electricity</td>
<td>NCF10-1</td>
</tr>
<tr>
<td>National Critical Function 11, Maintain Supply Chains</td>
<td>NCF11-1</td>
</tr>
<tr>
<td>National Critical Function 12, Transmit Electricity</td>
<td>NCF12-1</td>
</tr>
<tr>
<td>National Critical Function 13, Transport Cargo and Passengers by Air</td>
<td>NCF13-1</td>
</tr>
<tr>
<td>National Critical Function 14, Transport Cargo and Passengers by Rail</td>
<td>NCF14-1</td>
</tr>
<tr>
<td>National Critical Function 15, Transport Cargo and Passengers by Road</td>
<td>NCF15-1</td>
</tr>
<tr>
<td>National Critical Function 16, Transport Cargo and Passengers by Vessel</td>
<td>NCF16-1</td>
</tr>
<tr>
<td>National Critical Function 17, Transport Materials by Pipeline</td>
<td>NCF17-1</td>
</tr>
<tr>
<td>National Critical Function 18, Transport Passengers by Mass Transit</td>
<td>NCF18-1</td>
</tr>
<tr>
<td>National Critical Function 19, Conduct Elections</td>
<td>NCF19-1</td>
</tr>
<tr>
<td>National Critical Function 20, Develop and Maintain Public Works and Services</td>
<td>NCF20-1</td>
</tr>
<tr>
<td>National Critical Function 21, Educate and Train</td>
<td>NCF21-1</td>
</tr>
<tr>
<td>National Critical Function 22, Enforce the Law</td>
<td>NCF22-1</td>
</tr>
<tr>
<td>National Critical Function 23, Maintain Access to Medical Records</td>
<td>NCF23-1</td>
</tr>
<tr>
<td>National Critical Function 24, Manage Hazardous Materials</td>
<td>NCF24-1</td>
</tr>
<tr>
<td>National Critical Function 25, Manage Wastewater</td>
<td>NCF25-1</td>
</tr>
<tr>
<td>National Critical Function 26, Operate Government</td>
<td>NCF26-1</td>
</tr>
<tr>
<td>National Critical Function 27, Perform Cyber Incident Management Capabilities</td>
<td>NCF27-1</td>
</tr>
<tr>
<td>National Critical Function 28, Prepare for and Manage Emergencies</td>
<td>NCF28-1</td>
</tr>
<tr>
<td>National Critical Function 29, Preserve Constitutional Rights</td>
<td>NCF29-1</td>
</tr>
<tr>
<td>National Critical Function 30, Protect Sensitive Information</td>
<td>NCF30-1</td>
</tr>
<tr>
<td>National Critical Function 31, Provide and Maintain Infrastructure</td>
<td>NCF31-1</td>
</tr>
<tr>
<td>National Critical Function 32, Provide Capital Markets and Investment Activities</td>
<td>NCF32-1</td>
</tr>
<tr>
<td>National Critical Function 33, Provide Consumer and Commercial Banking Services</td>
<td>NCF33-1</td>
</tr>
<tr>
<td>National Critical Function 34, Provide Funding and Liquidity Services</td>
<td>NCF34-1</td>
</tr>
<tr>
<td>National Critical Function 35, Provide Identity Management and Associated Trust Support Services</td>
<td>NCF35-1</td>
</tr>
<tr>
<td>National Critical Function 36, Provide Insurance Services</td>
<td>NCF36-1</td>
</tr>
<tr>
<td>National Critical Function 37, Provide Medical Care</td>
<td>NCF37-1</td>
</tr>
</tbody>
</table>
National Critical Function 38, Provide Payment, Clearing, and Settlement Services .......... NCF38-1
National Critical Function 39, Provide Public Safety ...................................................... NCF39-1
National Critical Function 40, Provide Wholesale Funding ........................................... NCF40-1
National Critical Function 41, Store Fuel and Maintain Reserves ................................... NCF41-1
National Critical Function 42, Support Community Health ........................................... NCF42-1
National Critical Function 43, Exploration and Extraction of Fuels ................................ NCF43-1
National Critical Function 44, Fuel Refining and Processing Fuels ............................... NCF44-1
National Critical Function 45, Generate Electricity ..................................................... NCF45-1
National Critical Function 46, Manufacture Equipment ................................................ NCF46-1
National Critical Function 47, Produce and Provide Agricultural Products and Services .... NCF47-1
National Critical Function 48, Produce and Provide Human and Animal Food Products and
Services ................................................................. NCF48-1
National Critical Function 49, Produce Chemicals ....................................................... NCF49-1
National Critical Function 50, Provide Metals and Materials ......................................... NCF50-1
National Critical Function 51, Provide Housing ........................................................... NCF51-1
National Critical Function 52, Provide Information Technology Products and Services .......... NCF52-1
National Critical Function 53, Provide Materiel and Operational Support to Defense ........ NCF53-1
National Critical Function 54, Research and Development .......................................... NCF54-1
National Critical Function 55, Supply Water ................................................................. NCF55-1
APPENDIX B

Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

In this appendix, we provide the assessments for the 55 NCFs.
National Critical Function 1, Operate Core Network

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>The scope includes only a small number of high-capacity tier 1 network providers.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Strong, existing communities of practice, industry groups, and standard-setting bodies provide technical support and information-sharing that will help mitigate risk.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories and strong risk-mitigating factors lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)
Networks should make plans to implement post-quantum cryptography (PQC) where public-key cryptography is used to authenticate routing information using the border gateway protocol.

CISA definition: “Maintain and operate communications backbone infrastructure for voice, video, and data transmission that connects to users through broadcasting, cable, satellite, wireless, and wireline access networks” (CISA, 2020b, p. 2).

Synopsis of Issues
The functional scope of National Critical Function (NCF) 1 overlaps strongly with two other NCFs in the Connect category: NCF 2, Provide Cable Access Network Services, and NCF 4, Provide Internet Routing, Access, and Connection Services. However, the physical scope of NCF 1 is limited to the very high-bandwidth capabilities connecting large, regional network providers (nationally or internationally). Providers of this level of networking focus solely on transmission of data between access networks that ultimately fill the role of distribution to end-user devices. They are termed tier 1 Internet service providers for their role in enabling core or backbone connectivity (Greene, 2020; ThousandEyes, undated). Even so, the character of their vulnerabilities is largely shared with NCF 2 and NCF 4.

The NCF has a central role in the transmission of encrypted traffic across fiber networks, and those data include digital broadcast television, digital telephone services, and broadband Internet traffic. If sensitive data are transmitted over a cable network, the sender and receiver endpoints, not the core network operators, are those with the primary responsibility for the encryption operations on those data. In its own operations, the NCF does not use or control data with a long confidentiality lifetime, so it presents no clear catch-and-exploit vulnerabilities.

The major issues with this NCF are associated with vulnerabilities in authentication for network access. Such organizations as Internet service providers, businesses, and government organizations that maintain the backbone Internet routing infrastructure will need to migrate to PQC in the services that provide secure remote access to their networks. Security protocols used in the routers and other hardware used to direct Internet traffic will also need to adopt PQC, and this could be costly and challenging if adopting PQC negatively affects router performance. The intentionally distributed nature of the routing network is, however, somewhat resilient to disruptions in individual network providers (U.S. Department of Homeland Security [DHS], 2009). This NCF has been the focus of cyberattacks in the past, primarily incidents involving the border gateway protocol, the Internet interconnection protocol used to route Internet traffic. It is currently recommended that electronic communication providers implement public-key infrastructure (PKI) to
authenticate the routing system with digital signatures (Koukounas, Vytogianni, and Dekker, 2019). Wherever PKI is used in this manner, it will require replacement with quantum-resistant PKI.

Urgency
Our assessment is that urgency of action for this NCF is low. No catch-and-exploit issues are apparent, and it is unlikely any of the authentication vulnerabilities will be extensive or challenging enough to necessitate urgent attention. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low. Nationally, approximately ten organizations provide core network operations for the Internet backbone (Greene, 2020). Appropriate actions from organizations in this NCF are likely to happen over time with limited engagement.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, migration is likely to take place through software updates, security patches, and in-cycle hardware replacement for organizational network access. Depending on PQC hardware requirements, extensive replacements of routing hardware might be required, but the lack of urgency should allow these replacements in regular hardware refresh cycles. Additionally, required testing for new quantum-resistant methods will likely occur within the scope of current capabilities for deployment of upgraded infrastructure.

Other Factors
Our assessment is that other factors for this NCF are mitigating. The NCF has multiple large, existing organizations and communities of practice that set standards and provide information-sharing venues for guidance, technical support, and technical coordination of activities. Among the many entities involved are industry groups, such as the North American Network Operators’ Group (NANOG), the Internet Society (which supports the Mutually Agreed Norms for Routing Security [MANRS]), technical groups, and standard-setting bodies, such as the Internet Engineering Task Force. Although some R&D might be necessary to determine how to deploy changes to minimize wide-area disruptions, these activities will likely be supported by the community of providers. Because the NCF includes connectivity between a variety of access providers, such as radio access networks, the NCF’s integrity necessarily relies on the security of other NCFs in the Connect category. However, the information-sharing and technical coordination available from these groups and communities of practice, combined with the inherent resilience stemming from the distributed nature of the NCF, create strong risk-mitigating factors for this NCF.

Priority for Assistance
We rated the NCF as a low priority for assistance because of the consistently low ratings in each category and the presence of other strong risk-mitigating factors.

References
Works That Informed the Analysis


ThousandEyes, “ISP Tiers: Internet Service Provider 3-Tier Model,” webpage, undated.

Van Deynse, David, “Certificates and Different PKIs in DOCSIS 3.1,” *Excentis*, July 17, 2015.


**Related Reading**


National Critical Function 2, Provide Cable Access Network Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Urgency</th>
<th>Scope</th>
<th>Cost</th>
<th>Other factors</th>
<th>Priority for assistance</th>
<th>Primary concern(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Mitigating</td>
<td>Medium</td>
<td>Network providers must adopt post-quantum cryptography (PQC) to secure network access. A significant amount of hardware is likely to be affected, and costs for updates could be substantial.</td>
</tr>
</tbody>
</table>

Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.
Certificate authorities, hardware manufacturers, network operators, and other organizations all likely need to address vulnerabilities.
Updates will likely include large-scale deployments of new software or certificates to devices and industrywide hardware development and procurement.
The national critical function (NCF) has strong organizational support, and these organizations have been proactive in developing solutions to the issues affecting the NCF.

Despite mitigating factors, the expected scope and cost of updates lead to a rating of medium priority for assistance.

CISA definition: “Provide access to communications backbone infrastructure through fiber and coaxial cable network, supplying analog and digital video programming services, digital telephone service, and high-speed broadband services” (CISA, 2020b, p. 2).

Synopsis of Issues

The issues affecting this NCF overlap significantly with NCF 9, Provide Wireline Access Network Services, which covers the so-called last mile of wired network access. The assessment and context for this NCF are therefore largely identical to those for NCF 9.

The NCF has a role in the transmission of encrypted traffic across fiber and coaxial cable networks, and those data include digital broadcast television, digital telephone services, and broadband Internet traffic. If sensitive data are transmitted over a cable network, the sender and receiver endpoints, not the cable network operators, are those with primary responsibility for the encryption operations on those data. To prevent a network user from reading traffic that was not already encrypted, cable network operators also often encrypt traffic flows between individual modems and its terminal network system (CableLabs, 2017). That encryption is not a significant vulnerability with respect to quantum computing, however, because it uses symmetric-key cryptography. In its own operations, the NCF also does not use or control data with a long confidentiality lifetime, so it presents no clear catch-and-exploit vulnerabilities.

The NCF will experience significant authentication vulnerabilities in its operations due to extensive use of vulnerable public-key infrastructures (PKIs), as dictated by industrywide specifications, especially Data over Cable Service Interface Specifications (DOCSIS). The industry uses a chain of digital certificates to identify cable modems at endpoints (e.g., users, content providers, operator hardware) and control access to the network for those modems. At production time, every modem has a certificate installed for the device and another for the manufacturer. Other certificates are used to validate software and firmware updates to modems and routing hardware (Van Deynse, 2015). An attacker with a quantum computer could exploit the vulnerability in these certificates at multiple points in this chain (root certificate authority, trusted manufacturer, operator, or device), unless each of these certificates is replaced with a quantum-resistant version. This exploitation capability would allow the attacker to gain access to devices and operator networks or install
Preparing for Post-Quantum Critical Infrastructure

software onto a network. Finally, vulnerabilities in PKI used to secure routing messages using the border gateway protocol (BGP) would also present vulnerabilities for this NCF, although this is a more relevant issue for NCF 4, Provide Internet Routing, Access, and Connection Services, than for other NCFs.

Urgency
Our assessment is that urgency of action for this NCF is low. No catch-and-exploit issues are apparent, and it is unlikely that any of the authentication vulnerabilities will be extensive or challenging enough to necessitate urgent attention. The most-significant authentication vulnerabilities are those that would allow an attacker to impersonate a root certificate authority or trusted manufacturer to control hardware or perform widespread dissemination of malicious software. Before a quantum computer arrives, those organizations must transition to certificates that use PQC. Although vulnerable cryptographic systems are typically embedded in hardware at production and that hardware can be in use for long durations (i.e., 20 or more years), mechanisms exist for gradually addressing those vulnerabilities after deployment (Pala, 2020; Van Deynse, 2015). Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

Scope
Our assessment is that scope for this NCF is high. Standard-setting bodies, certificate authorities, hardware manufacturers, and network operators are all likely to require varying degrees of active engagement to address quantum computing vulnerabilities.

Cost
Our assessment is that cost per organization for this NCF is high. Many mitigation actions are likely to be straightforward, centralized actions that are massive in scope. For example, certificate authorities might need to deploy and sign hundreds of millions of new certificates, or operators and manufacturers might need to employ multiple strategies to remotely deploy upgrades to different classes of fielded devices while ensuring backward compatibility (Pala, 2020; Van Deynse, 2015). Other mitigation actions will require hardware work-arounds or redesigns that will need to be developed and tested according to newly developed specifications. Where work-arounds are inadequate and PQC deployment creates performance bottlenecks, new hardware might need to be acquired (Pala, 2021).

Other Factors
Our assessment is that other factors for this NCF are mitigating. The industry is aware of the vulnerabilities from quantum computing and proactively working to address them. Documented activities include planned updates to industrywide specifications, such as DOCSIS, creation of new cryptographic libraries, and ongoing investigation of the operational challenges that PQC could create (Pala, 2020; Pala, 2021; Stebila and Mosca, 2017). The NCF as a whole is well supported by government and industry organizations, such as CableLabs, Excentis, the Open Connectivity Foundation, the Broadband Internet Technical Advisory Group, and the Communications Security, Reliability, and Interoperability Council of the Federal Communications Commission. Finally, the distributed, redundant nature of connections between cable networks is likely to make them resilient to a broader disruption from attacks on single network providers, like with other network access NCFs (e.g., NCF 4) (DHS, 2009).

Priority for Assistance
We rated the NCF as a medium priority for assistance. Organizations in this NCF likely have the industry support needed to understand the problems affecting them and the solutions to those problems. The cost for
implementing those solutions is likely to be substantial, however, and the scope of affected organizations is broad.

References

Works That Informed the Analysis
Van Deynse, David, “Certificates and Different PKIs in DOCSIS 3.1,” Excentis, July 17, 2015.

Related Reading
National Critical Function 3, Provide Internet Based Content, Information, and Communication Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
</tr>
<tr>
<td>Cost</td>
<td>Medium</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>High</td>
</tr>
</tbody>
</table>

The national critical function (NCF) handles a significant amount of data in transit with a long confidentiality lifetime. Authentication vulnerabilities might also not be fully addressed in time.

Most of the organizations providing products and services that are Internet based must individually address updates.

Cost will vary significantly from organization to organization in this NCF, but the majority of the affected organizations will likely need substantial software development, at a minimum.

The NCF has both exacerbating and mitigating factors, but the balance is exacerbating. The organizations in the NCF are already experiencing significant cybersecurity vulnerabilities, and many other NCFs are highly dependent on the products and services delivered by this NCF. The NCF will benefit, however, from significant proactive work already occurring to facilitate the migration to post-quantum cryptography (PQC).

The NCF has a high urgency, massive scope, and exacerbating factors. Many organizations in the NCF will benefit from assistance, although some of the largest will not.

- Many Internet-based products and services handle data with a long confidentiality lifetime, and they must implement new PQC standards for key exchange as soon as practical.
- Migrations to new standards have historically taken decades, and it is imperative that this NCF be supported in expeditiously beginning the PQC transition.

CISA definition: “Produce and provide technologies, services, and infrastructure that deliver key content, information, and communications capabilities via the Internet” (CISA, 2020b, p. 2).

Synopsis of Issues

This NCF is one of those most affected by the vulnerabilities from quantum computers. The NCF spans the gamut of services that use the Internet to securely collaborate and share information. It has subfunctions providing national security emergency preparedness and law enforcement functions; critical web search capabilities, including mapping and geospatial data and imagery services; e-commerce and financial transaction services; and communication and collaboration services. The communication and collaboration services include video voice over Internet protocol, peer-to-peer file-sharing, email, instant messaging, and supervisory control and data acquisition (SCADA) communication (U.S. Department of Homeland Security [DHS], 2009). Moreover, the organizations involved are typically not merely passive handlers of encrypted sensitive information but are often the ones providing the platforms, applications, and services that handle the encryption and secure transmission of sensitive data. Given the centrality of issues affecting software applications and remote identity management in this NCF, many of the issues discussed here overlap significantly with those in NCF 35, Provide Identity Management and Associated Trust Support Services, and NCF 52, Provide Information Technology Products and Services.

This NCF is a critical enabling function for the secure communication of sensitive data using the Internet and has at least partial responsibility for the significant majority of the conceivable examples of catch-and-exploit vulnerabilities, with examples too varied and numerous to list. The use of the Internet is so ubiquitous that almost every identifiable category of data in transit with a long confidentiality lifetime will likely use an
Preparing for Post-Quantum Critical Infrastructure

Internet-based communication or collaboration tool in some way. Every organization that provides a product or service that uses the Internet to facilitate the transmission of these data will need to migrate that product or service to PQC as soon as it is practical. The organizations in this NCF will be the providers on which organizations in other NCFs depend to quickly create the updated tools needed to secure Internet-based data transmissions against catch-and-exploit vulnerabilities. The urgency and priority of migration will depend on the confidentiality lifetime of the data used in that application.

Nearly every current instance of a presumed secure interaction on the Internet will present an authentication vulnerability when a cryptographically relevant quantum computer (CRQC) exists. The primary authentication vulnerabilities affecting this NCF stem from the ubiquitous use of public-key infrastructures (PKIs) to identify entities on the network. Although some aspects of PKI are more appropriately described in the discussion of NCF 35, Provide Identity Management and Associated Trust Support Services, the use of digital signatures and digital certificates are of particular relevance to the authentication vulnerabilities in this NCF. Digital signatures and certificates use public-key cryptography to identify entities on the network and confirm authenticity in online interactions. Quantum computing will enable an attacker to derive the private cryptographic keys associated with these tools, allowing the attacker to falsely identify itself as nearly any user or organization on the Internet. Every instance in which hypertext transfer protocol secure (HTTPS) is currently used in a web browser application uses digital certificates to facilitate the secure interaction. This would include notable examples, such as secure financial transactions for e-commerce or online forms involving communication of personally identifiable information (PII), such as social security numbers and medical information, along with many other scenarios requiring secure web browsing. The category of browser-based vulnerabilities likely makes up a significant portion of the authentication vulnerabilities. Any other stand-alone (i.e., not accessed through a web browser) software applications that enable secure connections over the Internet will also be vulnerable, including applications for virtual private networks (VPNs), email, video calls, file-sharing, messaging, and SCADA communication. The vulnerability in these applications would extend beyond an attacker impersonating a user and would include a case in which an attacker impersonates an owner of a service or product itself. This could, for example, allow an attacker to disguise malware as a trusted secure update for users (see Stiennon, 2012). Finally, the vulnerability would also extend to the entire ecosystem of applications enabled by the cloud, which depends on digital certificates and digital signatures to authenticate user access. This includes storage, software as a service, and key management. The most troubling of the vulnerabilities described here are those that have the capacity to have systemic security impacts across the Internet ecosystem, such as if an attacker exploited a vulnerability to receive root access to databases of other cryptography keys held in the cloud (e.g., database read–write keys held in Microsoft’s Azure Cosmos DB database; see Menn, 2021).

Urgency

Our assessment is that urgency of action for this NCF is high. A significant portion of the conceivable examples of catch-and-exploit vulnerabilities likely use the Internet in some way to facilitate the transmission of sensitive data. Every such instance that involves data with a long confidentiality lifetime (and these are likely myriad) will need to move to a post-quantum algorithm for key establishment in communications as soon as possible to limit the risk incurred by the vulnerability.

Providers of products and services that use digital certificates and PKI to authenticate users and organizations on the Internet will need to move to PQC only before a CRQC is available to attackers. The migration to new standards across the Internet is historically long and slow, however, and many unaddressed authentication vulnerabilities might still be in place when that time comes (Vermeer and Peet, 2020). If the move to PQC is not prioritized among the many product and service providers across this NCF, it might not yet be possible to more broadly deprecate old, vulnerable standards when a CRQC arrives. Authentication issues
therefore also contribute to an assessment of a high urgency for this NCF; organizations should begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Finally, other NCFs will depend on this NCF to rapidly produce the shared resources needed to begin a broader migration to PQC across the Internet ecosystem. These resources include updates to standards for digital certificates and digital signatures (e.g., X.509), widely used communication protocols in different layers of the Internet protocol suite (e.g., HTTPS, transport-layer security [TLS], Internet protocol security [IPsec], Secure/Multipurpose Internet Mail Extensions [S/MIME]), updated cryptographic libraries, and configuration guidance. It is imperative that the protocols, cryptographic libraries, and other shared resources needed to facilitate the migration to PQC be ready as soon as practical after the National Institute of Standards and Technology (NIST) releases the standard PQC algorithms.

Scope
Our assessment is that scope for this NCF is high. Nearly every organization that uses the Internet to deliver a product or service will be required to make an update to address vulnerabilities. Providers of web browsers, cloud service providers, and certificate authorities will be among the members of this scope with the most systemic impact. Beyond these, every organization that uses PKI and the Internet to provide some content, information, or communication service will need to update its product to enable the use of PQC in secure online interactions.

Cost
Our assessment is that cost per organization for this NCF is medium overall. There will likely be significant variation in this category, with very high costs borne by those required to migrate early and diminishing costs borne by those who are able to migrate later. It will likely be necessary to use hybrid schema that combine conventional cryptography and PQC algorithms and the formats, and requirements for these schema are still being developed and tested (see Crane, 2020; Truskovsky et al., 2018). The post-quantum algorithms under consideration by NIST are also generally more computationally demanding to use (Kwiatkowski and Valenta, 2019), and this could have significant cost implications where system performance requirements are high.

Organizations that produce some of the most–widely used web browsers, enterprise communication and collaboration products, and cloud-based services will likely be at the vanguard of the migration to PQC and incur very high costs. Many of these products and services are highly complex and have strict business requirements for performance, interoperability, and cybersecurity. They will require extensive software development, testing in real network conditions, and potentially new hardware acquisition to facilitate the successful migration to PQC (see, for example, Cimpanu, 2021; Paquin, Stebila, and Tamvada, 2020; and Weibel, 2020).

Most of the products and services in the NCF that are not in the top tier in terms of distribution and complexity are also likely to incur medium to high costs, depending on the application. They will likely need significant software development and testing to accommodate new formats, protocols, and processing requirements for post-quantum digital certificates, key exchange, and digital signatures. Where fast processing and reduced latency in connections are required, new hardware acquisitions might be needed, especially in the situations in which catch-and-exploit vulnerabilities necessitate a faster migration.

The remaining organizations that have less urgency to migrate to PQC will likely benefit from the work of the first movers. They will likely be able to follow established guidance, use publicly available cryptographic libraries, and acquire the necessary hardware in routine refresh cycles. Many will still likely need to perform some software development to migrate their products and services to PQC, but, in some cases, the
updates may be minimal (e.g., enabling the use of alternative security configurations or new digital certificate formats).

Other Factors
Our assessment is that other factors for this NCF are exacerbating, on balance, although some mitigating factors are present. Identified exacerbating factors include the following:

- This NCF is already vulnerable to conventional cyberattacks because of its constant accessibility and exposure, and attackers with a variety of motivations and capabilities are already regularly exploiting those vulnerabilities (DHS, 2009). The quantum vulnerabilities in this NCF will be layered on top of existing conventional vulnerabilities, adding new attack vectors and requiring additional complexity in the systems used to defend.
- Many other NCFs are highly dependent on this NCF. Delays in migration to PQC and the provision of products and services that facilitate quantum-safe communication and collaboration will create enduring vulnerability in other NCFs that use those products and services. Moreover, these vulnerabilities will affect one of the roots of trust in the Internet ecosystem. Attacks have the potential to lead to further compromise in many other connected systems, leading to broader disruptions and impacts that cascade to end users. This statement about the NCF in DHS, 2009, applies to the quantum vulnerabilities in this NCF:

> The concerns are broadly applicable because video VoIP [voice over Internet protocol], e-mail, IM [instant message], P2P [peer to peer], and other services play an integral part in the daily operations of many organizations. This level of connectivity to and reliance upon the Internet ensures that the impact of a successful attack on the function cascades to the end user. . . . Additionally, it could take months to notice that vulnerabilities were being exploited, which can lead to significant revenue and intellectual property losses. (p. 51)

The challenging issues in this NCF are nevertheless also mitigated to a degree by the many effective organizations (governmental, nongovernmental, and commercial) that have already been proactively involved for years in addressing the known vulnerabilities. Among the most important are organizations that have been actively developing the specifications and guidelines for the agile incorporation of PQC into the security of the Internet (see, for example, the draft Internet Engineering Task Force document describing hybrid key exchange schema for transport-layer security [TLS] 1.2, Campagna and Crockett, 2021). Many organizations in this ecosystem have been performing research and development to prepare in their respective domains, often directly collaborating with NIST in the standardization process. Their proactive work will likely provide a crucial starting point for other organizations in the NCF.

Priority for Assistance
We rated the NCF as a high priority for assistance. Many of the large companies that provide distributed information technology infrastructure (e.g., web browsers, cloud services, enterprise communication and collaboration tools) have been engaged on the problem for years and are unlikely to benefit from technical assistance from the U.S. government. Many organizations, however, do not fall into that category. Examples might include providers of content delivery network software, collaboration and communication tools, and the myriad other types of products delivered as software as a service. These others will benefit from the early, proactive work of these organizations in understanding the challenges and creating the specifications, standards, protocols, and guidance needed to migrate, but they will also likely benefit from support in prioritizing and managing the migration following the steps outlined in the DHS roadmap for PQC migration. They
will need to understand the importance of the issue (especially if they handle data with a long confidentiality lifetime); they will need guidance and resources to manage the software, hardware, or configuration changes needed for the migration; and they might need other incentives or certification regimes to overcome concerns about cost or impacts on performance and interoperability.

References

Works That Informed the Analysis


DHS, Information Technology Sector Baseline Risk Assessment, August 2009.


Related Reading


Loshin, Peter, and Mike Chapple, “How to Encrypt and Secure a Website Using HTTPS,” webpage, TechTarget, undated.
National Critical Function 4, Provide Internet Routing, Access, and Connection Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Strong, existing communities of practice, industry groups, and standard-setting bodies provide technical support and information-sharing that will help mitigate risk.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories and strong risk-mitigating factors lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s): Networks should make plans to implement post-quantum cryptography (PQC) where public-key cryptography is used to authenticate routing information using the border gateway protocol.

CISA definition: “Provide and operate exchange and routing infrastructure, points of presence, peering points, local access services, and capabilities that enable end users to send and receive information via the Internet” (CISA, 2020b, p. 3).

Synopsis of Issues

Although the national critical function (NCF) has a role in the secure transmission of data across the Internet, it is primarily responsible for managing layers of the communication infrastructure below the application layer (and below the presentation layer in the Open Systems Interconnection [OSI] model) and therefore does not generally have responsibility for whether and how Internet traffic is encrypted. In its own operations, the NCF also does not use or control data with a long confidentiality lifetime, so it presents no clear catch-and-exploit vulnerabilities.

The major issues with this NCF are associated with vulnerabilities in authentication for network access. Such organizations as Internet service providers, businesses, and government organizations that maintain the backbone Internet routing infrastructure will need to migrate to PQC in the services that provide secure remote access to their networks. Security protocols used in the routers and other hardware used to direct Internet traffic will also need to adopt PQC, and this could be costly and challenging if adopting PQC negatively affects router performance. The intentionally distributed nature of the routing network is, however, somewhat resilient to disruptions in individual network providers (U.S. Department of Homeland Security [DHS], 2009). This NCF has been the focus of cyberattacks in the past, primarily incidents involving the border gateway protocol, the Internet interconnection protocol used to route Internet traffic. It is currently recommended that electronic communication providers implement public-key infrastructure (PKI) to authenticate the routing system with digital signatures (Koukounas, Vytogianni, and Dekker, 2019). Whenever PKI is used in this manner, it will require replacement with quantum-resistant PKI.

Urgency

Our assessment is that urgency of action for this NCF is low. No catch-and-exploit issues are apparent, and it is unlikely that any of the authentication vulnerabilities will be extensive or challenging enough to neces-
sitate urgent attention. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**
Our assessment is that scope for this NCF is low because situations requiring active, swift risk mitigation are likely to be rare. Appropriate actions from organizations in this NCF are likely to happen over time with limited engagement.

**Cost**
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, migration is likely to take place through software updates, security patches, and in-cycle hardware replacement for organizational network access. Depending on PQC hardware requirements, extensive replacements of routing hardware might be required, but the lack of urgency should allow these to be made in regular hardware refresh cycles.

**Other Factors**
Our assessment is that other factors for this NCF are mitigating. The NCF has multiple large, existing organizations and communities of practice that set standards and provide information-sharing venues for guidance and technical support. These include industry groups, such as the North American Network Operators’ Group (NANOG), the Internet Society (which supports Mutually Agreed Norms for Routing Security [MANRS]), technical groups, and standard-setting bodies, such as the Internet Engineering Task Force. The information-sharing and technical support available from these groups and communities of practice, combined with the inherent resilience stemming from the distributed nature of the NCF, create strong risk-mitigating factors for this NCF.

**Priority for Assistance**
We rated the NCF as a low priority for assistance because of the consistently low ratings in each category and the presence of other strong risk-mitigating factors.

**References**

Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.

Related Reading
National Critical Function 5, Provide Positioning, Navigation, and Timing Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
<th>We identified no catch-and-exploit vulnerabilities, and authentication vulnerabilities will likely be addressed before a capable quantum computer exists.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>A few centralized positioning, navigation, and timing (PNT) service providers will need to act to adopt post-quantum cryptography (PQC).</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Most organizations will incur little cost because they will benefit from PQC migration efforts happening in other national critical functions (NCFs).</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>Mitigating and exacerbating factors are present. Practical considerations of exploiting vulnerabilities make broader disruptions unlikely, but performance impacts of PQC adoption could delay broader implementation.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a low rating in priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Centralized sources of PNT services need to adopt PQC to protect remote access to their networks.

CISA definition: “Operate and maintain public and private capabilities which enable users to determine location, orientation and time” (CISA, 2020b, p. 3).

Synopsis of Issues

The NCF does not handle data with a long confidentiality lifetime and therefore will not experience any catch-and-exploit vulnerabilities.

Authentication vulnerabilities for this NCF will exist in mechanisms for providing security at points of transmission of PNT services, at points of receipt, and in any encrypted delivery of PNT services. The most-significant authentication issues involve the use of public-key infrastructure for authenticated communications between PNT service providers and users. Examples would include authentication in Internet-based timing services (e.g., the network time protocol; see O’Donoghue, 2017) and any authenticated navigation services, such as commercial or government services used in vehicle and aviation navigation. PNT provider networks that allow remote access through virtual private networks (VPNs) or public-key infrastructure will be vulnerable until PQC is implemented. Any remotely accessible hardware used for transmission or receipt of PNT services (e.g., networked global navigation satellite system [GNSS] receivers) will similarly need to adopt PQC to avoid authentication vulnerabilities. Some of the issues involving satellite PNT systems, such as the Global Positioning System, overlap with NCF 7, Provide Satellite Access Network Services, and are discussed in more detail in that NCF’s assessment.

Urgency

Our assessment is that urgency of action for this NCF is low. We identified no catch-and-exploit vulnerabilities. We expect that authentication vulnerabilities will be able to be addressed before a capable quantum computer exists. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.
Scope
Our assessment is that scope for this NCF is low. Despite the widespread use of PNT services throughout critical infrastructure (see CISA, undated d), scope is low because many PNT services are not authenticated with public-key cryptography, and many of the most-widely used services are provided by just a few primary sources. For those PNT services that are authenticated with public-key cryptography, situations requiring active, swift risk mitigation are likely to be rare in this NCF. Appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, utilizing such resources as freely available cryptographic libraries, new communication protocol versions (e.g., transport-layer security [TLS]), and updated information technology products made available from other NCFs.

Cost
Our assessment is that cost per organization for this NCF is low. Although there will be a few specific cases in which adopting PQC in authentication for PNT sources could require significant development and implementation cost (e.g., U.S. Department of Defense use of the Global Positioning System [GPS] Precise Positioning Service; see National Coordination Office for Space-Based PNT, 2020), most PNT providers will require no action or will benefit from migration actions associated with other NCFs, such as the adoption of PQC in Internet-based communications.

Other Factors
Our assessment is that other factors for this NCF are neutral, with both mitigating and exacerbating factors identified. As a mitigating factor, many current vulnerabilities in the NCF are associated with an attacker exploiting unsecured PNT sources to spoof PNT data (U.S. Department of the Treasury et al., 2015) or for other purposes unrelated to disruption of the PNT service itself (e.g., distributed denial-of-service attacks) (Snoke, 2017). Using a quantum computer to exploit vulnerable public-key cryptography in secured systems is likely to require significant resources at first, and broadly distributed PNT services will likely be protected before a cryptographically relevant quantum computer arrives. This means that, in most cases, an attacker would need to invest significant resources into attacking a relatively low-value target (e.g., a single global navigation satellite system [GNSS] receiver or network time protocol server), and attacks would be unlikely to lead to a broader degradation or disruption of the function, especially given the typical availability of multiple complementary sources for timing, in particular.

As an exacerbating factor, for PNT services, microseconds often matter. Latency reduction is often a critical performance measure when using PNT services, and the use of encryption can negatively affect performance (O’Donoghue, 2017). PQC is likely to require greater computational resources and lead to an even greater negative impact on performance than current cryptographic algorithms. Even for systems that rely on symmetric-key cryptography, the increased symmetric-key strength needed for protection against quantum computing could lead to performance impacts. These impacts could lead to delayed implementation of PQC or increased costs.

Priority for Assistance
We rated the NCF as a low priority for assistance due to low ratings in all categories.

References
Works That Informed the Analysis
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions


Related Reading

National Critical Function 6, Provide Radio Broadcast Access Network Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Situations requiring active, swift mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Migration is likely to take place through routine, conventional cybersecurity efforts, such as software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>Although the national critical function (NCF) is a frequent target of cyberattacks, it is well supported by an array of public and private organizations.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td></td>
<td>Organizational network access and operations that rely on Internet-based services must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
</tr>
</tbody>
</table>

CISA definition: “Operate over-the-air radio and television (TV) stations (operating at medium, very high, and ultra-high frequencies) that offer analog and digital audio and video programming services and data service” (CISA, 2020b, p. 3).

Synopsis of Issues

In rare instances in which the NCF might handle sensitive data, those data do not have a long confidentiality lifetime. We identified no catch-and-exploit issues.

Authentication vulnerabilities in the NCF relate to broadcasters’ reliance on Internet-based services in their operations (National Association of Broadcasters, 2016; Working Group 4, 2015), and they are therefore derived primarily from products and services delivered by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Broadcasters will experience authentication vulnerabilities in the public-key infrastructures (PKIs) used for Internet-based content delivery, cloud services, and other communications, as well as in the IT products and services that facilitate related operations. In the instances in which encryption is used to secure broadcasted data, transmissions use symmetric-key cryptography, and they are thus not considered a quantum computing vulnerability for this NCF (Security Working Group, 2016).

Urgency

Our assessment is that urgency of action for this NCF is low. Systems used to protect Internet-based network access, content delivery, and communication will need to migrate to PQC over time, but these systems need complete the migration only prior to the arrival of a cryptographically relevant quantum computer. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.
Preparing for Post-Quantum Critical Infrastructure

Scope
Our assessment is that scope for this NCF is low. Situations requiring active, swift risk mitigation are likely to be rare in this NCF. Appropriate actions from organizations in this NCF will be minor in scope and are likely to happen over time with limited engagement.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. Migration to PQC is likely to take place as part of routine, conventional cybersecurity efforts, such as software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are neutral on balance. The industry is a regular target of cyberattacks, with numerous recent examples (National Association of Broadcasters, 2016, p. 7). However, the NCF is also very well supported by an array of public and private organizations that will be beneficial in facilitating the industry’s migration to PQC. These include the Communications Security, Reliability, and Interoperability Council of the Federal Communications Commission, the Shared Resources High Frequency Radio program and the Interoperable Communications Technical Assistance Program of CISA, and the National Association of Broadcasters.

Priority for Assistance
We rated the NCF as a low priority for assistance due to low ratings in all categories.

References
Works That Informed the Analysis
National Critical Function 7, Provide Satellite Access Network Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>High</th>
<th>The national critical function (NCF) will experience catch-and-exploit vulnerabilities in terrestrial network links that require urgent action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Medium</td>
<td>There are likely between ten and 100 satellite communication network operators that must effect a migration to post-quantum cryptography (PQC).</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>The main changes needed are in key exchange and authentication in terrestrial network links, which are likely to need only low-cost updates.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>The NCF is well supported by government and industry associations. The strong influence of national security system (NSS) requirements on the industry as a whole is likely to provide a strong mitigating factor.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>Urgent changes are likely to be low cost, and the NCF as a whole is well supported.</td>
</tr>
</tbody>
</table>

Primary concern(s) Satellite network operators urgently need to implement PQC for key exchange in terrestrial network links to address catch-and-exploit vulnerabilities.

CISA definition: “Provide access to core communications network via a combination of terrestrial antenna stations and platforms orbiting earth to relay voice, video, or data signals” (CISA, 2020b, p. 3).

Synopsis of Issues

This NCF involves unique requirements and constraints on the use of encryption. Communications from satellite to satellite and between satellites and ground stations can be encrypted to secure satellite systems, protect information, and verify the authenticity of messages. Ground stations of communication networks use public-key infrastructures (PKIs) to connect to other terrestrial networks. Satellite communication networks can also act as routers of communications without performing cryptographic operations on the communications themselves. The use of encryption, especially public-key encryption, creates increased demands for computational power and message bandwidth. Although terrestrial systems can often meet these demands, a deployed satellite represents a highly constrained system, and alternative security and trust mechanisms are typically used in lieu of public-key cryptography (Cao et al., 2020; Littman, 2009; Manulis et al., 2021; Soper, 2009). These alternatives, especially the frequent use of symmetric-key encryption, will provide some innately better security against quantum computers, but the NCF might nevertheless be challenged by the negligible cryptographic agility in deployed satellite constellations.

The NCF is likely to experience significant catch-and-exploit vulnerabilities. Satellite communication networks are often used to transmit highly sensitive information with a long confidentiality lifetime, including national security-related communications. Catch-and-exploit vulnerabilities will most likely occur in the ground segments of the network. According to our analysis of available information, communications to and from satellites are presumed to use strong symmetric-key encryption in which sensitive information is transferred, and this will not represent a significant quantum computing vulnerability (Manulis et al., 2021). The exception to this would be where weaker security mechanisms are used with no feasible ability to update. Ground segments will use PKIs where they connect with other terrestrial networks and endpoints, and these will create catch-and-exploit vulnerabilities until those connections adopt PQC for key exchange.

Authentication vulnerabilities for the NCF will largely mirror those experienced by other communication network operators. An operator will be vulnerable where remote access to its internal network is enabled.
via such services as virtual private networks (VPNs) and in any other information technology products and services that use PKIs (e.g., cloud computing services). These vulnerabilities are derived primarily from products and services delivered by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Although authenticated communications to and from satellites use mechanisms that are presumed to be at least somewhat quantum resistant, authentication vulnerabilities might also exist where applications have not adapted to the increased key strengths needed to defend against quantum computers.

**Urgency**

Our assessment is that urgency of action for this NCF is high. The NCF handles data with a long confidentiality lifetime in both terrestrial and space-based communication links, and it is often responsible for the encryption and secure transmission of those data, rather than solely acting as a passive router of the data. It is likely that no catch-and-exploit vulnerability is present in applications in which those data stay within a single satellite network and associated ground segments. Radio links with satellites are typically protected with symmetric-key cryptography, and the authentication vulnerabilities in access to operator networks need to be addressed only before a cryptographically relevant quantum computer exists. Commercial satellite networks connect with other terrestrial networks, however, and vulnerable public-key cryptography is used to facilitate key exchange across those terrestrial networking links. In those cases, the NCF is responsible for securely transmitting data that might have a long confidentiality lifetime, and it is urgent that PQC be implemented quickly for key exchange. A secondary concern is that the constrained hardware environment in space-based systems can involve significant trade-offs between security and performance, and planning might need to begin quickly to ensure that systems being designed now will have sufficient cryptographic agility and avoid embedding systems with long-lived vulnerabilities. Organizations should begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**

Our assessment is that scope for this NCF is medium. From available data on satellite operators (Union of Concerned Scientists, 2021), we estimated that between ten and 100 separate organizations in this NCF operate satellites for communication purposes and will need to address quantum computing vulnerabilities in some way.

**Cost**

Our assessment is that cost per organization for this NCF is low overall, although some high-cost scenarios are possible. Because the primary issues that must be addressed quickly relate to terrestrial links with other networks and other Internet-based delivery of services, the cost to address these issues for operators providing this NCF is likely to be low. It will likely involve configuration changes or limited software changes based on existing standards and guidance, although organizations should begin to follow the preparation steps outlined in the DHS roadmap. It is possible that some scenarios will involve very high costs instead. Those cases would include significant hardware development and procurement to meet more-stringent security requirements with PQC in terrestrial network links (e.g., in which an application must meet new requirements for the Commercial National Security Algorithm Suite; see National Security Agency/Central Security Service [NSA/CSS], 2015) or hardware redesigns for the next generation of deployed satellites (e.g., where stronger keys or greater cryptographic agility are needed).
Other Factors
Our assessment is that other factors for this NCF are mitigating. Smaller satellite network operators find conventional cybersecurity needs challenging now, and the increased performance requirements for PQC could exacerbate this challenge (Werner, 2018). The importance of satellite communications to national security applications has resulted in much of the larger providers in the industry placing a high priority on cybersecurity in order to meet the NSA/CSS requirements for NSSs. As NSA/CSS requirements for NSSs adapt to include the new PQC standard (NSA/CSS, 2015; NSA/CSS, 2021), it is likely that much of the industry will follow suit with a broader migration to PQC. The industry is also well supported by other organizations, such as the Satellite Industry Association, the Federal Communications Commission, DHS, the National Institute of Standards and Technology [NIST], industry working groups, and international standard-setting bodies (Satellite Industry Association, undated). These factors are considered mitigating overall.

Priority for Assistance
We rated the NCF as a medium priority for assistance. The NCF must act quickly to address catch-and-exploit vulnerabilities in terrestrial network links, but links to and from satellites themselves are likely not an urgent concern. Cost per organization to address terrestrial link vulnerabilities are not expected to be high. Finally, NSA/CSS's significant influence in setting standards for large organizations providing NSSs in the satellite industry is also likely to be a strong mitigating factor. Overall, the NCF is a medium priority for assistance, and much of that assistance can be mediated via the existing organizational support for the NCF.

References
Works That Informed the Analysis
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.
National Critical Function 8, Provide Wireless Access Network Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>High</th>
<th>Data with a long confidentiality lifetime are currently transmitted with vulnerable encryption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
<td>Each network provider and device manufacturer will need to address vulnerabilities in its products and services.</td>
</tr>
<tr>
<td>Cost</td>
<td>Medium</td>
<td>Urgent hardware development and production are needed, but the required changes are likely to be small in scope and can use existing algorithms and standards.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Layered encryption in wireless data traffic and the practical difficulty in using a quantum computer to derive a symmetric key are strong mitigating factors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>The high ratings in urgency, scope, and cost are offset by strong mitigating factors to result in a medium priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Device manufacturers must begin to produce security modules that employ stronger cryptographic keys as soon as practicable to allow users to address catch-and-exploit vulnerabilities.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Provide access to core communications network via electromagnetic wave-based technologies, including cellular phones, wireless hot spots (Wi-Fi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services” (CISA, 2020b, p. 3).

Synopsis of Issues

This national critical function (NCF) will experience significant catch-and-exploit vulnerabilities, although it might be difficult for an attacker to take advantage of those vulnerabilities in practice. This NCF is responsible for the security of data in the wireless communication links between user devices (e.g., laptops, cellular phones) and network access points, such as Wi-Fi routers. In many cases, any sensitive Internet-facilitated traffic across those links will have already been encrypted by products and services in other NCFs that provide secure web connections (e.g., with hypertext transfer protocol secure [HTTPS] connections; associated issues are discussed along with the assessments of NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Other sensitive data that were not already encrypted will travel across these wireless network links (e.g., sensitive local network traffic that is not bound for the Internet), however, and these data will present a significant catch-and-exploit vulnerability. Wireless communications are typically secured with symmetric-key cryptography (Irei and Scarpati, 2020), which is relatively secure against quantum computers and would normally not be considered a vulnerability in these NCF assessments. Some data traveling across wireless links could have a very long confidentiality lifetime, however, and the symmetric keys used to secure wireless communications are typically weak enough that it would be challenging, but not impossible, for an attacker with a quantum computer to derive them (Mitchell, 2020).

Few authentication vulnerabilities currently exist in this NCF, although future technology generations might need to address additional vulnerabilities. Networks typically identify connected equipment via physical, often card-based, assets shared with users (e.g., subscriber identity module cards in cellular phones or modules preinstalled in devices). Although weak symmetric keys could present a catch-and-exploit vulnerability in some cases, they do not present a significant authentication vulnerability; it will likely be trivial to strengthen these symmetric keys sufficiently to make an attack impractical by the time a quantum computer exists. Some security mechanisms, especially those used in fifth-generation (5G) networks, use public key–
based authentication to identify equipment, and these will present an authentication vulnerability until they adopt post-quantum cryptography (PQC) (Mitchell, 2020).

**Urgency**

Our assessment is that urgency of action for this NCF is high. Data with a long confidentiality lifetime are likely being transmitted, now secured by symmetric keys that can feasibly be obtained by an attacker with a cryptographically relevant quantum computer. These keys are intended to provide long-term security for devices, and, if one were obtained by an attacker, all past and future voice and data traffic from the device could be read. On occasion, providers have also used root keys to create all the keys distributed to user devices. If the key strength were weak enough that a quantum computer could feasibly derive it, the catch-and-exploit vulnerability would extend to traffic from every device whose key was derived from the root key (Mitchell, 2020).\(^1\) Symmetric-key strength needs to be increased to an adequate level (i.e., 256 bits) as soon as practical in any application in which sensitive data with a long confidentiality lifetime might be transmitted. The vulnerable public-key infrastructures introduced in 5G infrastructure will also need to adopt PQC, but those vulnerabilities must be addressed only before a capable quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**

Our assessment is that scope for this NCF is high. The scope includes the providers of wireless networks and every manufacturer of a device equipped with wireless network access capability. Just by those criteria, the scope would include well over 100 organizations (FactSet, 2021), meeting the criteria for a high scope. Each of these organizations will need to take action to enable the use of strong symmetric keys in wireless communications and, where applicable, post-quantum public-key infrastructures for device authentication.

**Cost**

Our assessment is that cost per organization for this NCF is medium. Required actions across the NCF would be largely defined by the production of new installable or hardware-embedded security modules. These modules could use the same standards and algorithms as those currently in use but would use stronger keys than the current standard. According to assessment criteria, the urgent development of novel hardware would normally be classified as a high-cost scenario, but the simplicity of the change needed leads instead to a rating of medium for cost per organization.

Per Mitchell, 2020, a significant portion of the vulnerability for the current generation of devices could be obviated if the relevant standard for device keys were “trivially changed” to allow 256-bit device keys,\(^2\) followed by manufacturers moving to issue all new device keys with 256 bits instead of 128 bits. As Mitchell described, “changing the entire system to use 256-bit keys will require more far-reaching changes to the system (covering the network infrastructure and handsets)” (Mitchell, 2020, p. 9), but characteristics of the infrastructure should make that change feasible while maintaining backward compatibility. Fortunately, this migration would not need to wait until the National Institute of Standards and Technology releases a PQC standard because existing, standardized symmetric-key algorithms are quantum resistant.

---

\(^1\) It is not known whether any network currently uses this practice to manage device keys, although the practice was used in the past (Mitchell, 2020).

\(^2\) This change has since happened in the relevant standard. See 3rd Generation Partnership Project (3GPP), 2018.
Other Factors
Our assessment is that other factors for this NCF are mitigating. In many cases involving access to the Internet, any sensitive data sent over wireless links will have already been encrypted by applications that provide secure web connections (e.g., with HTTPS connections; associated issues are discussed in assessments for NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). In many cases, therefore, this NCF is only responsible for providing an additional layer of encryption that is already quantum resistant in its current form (Mitchell, 2020). Changes to the 5G standards to allow 256-bit symmetric keys also indicate that the industry is already taking steps toward the necessary cryptographic agility in preparation for quantum computers (3GPP, 2018).

The strongest mitigating factor, however, is the significant practical difficulty of carrying out an impactful catch-and-exploit campaign on data protected by symmetric-key cryptography. Even if an adversary with a quantum computer knew which devices were being used to route targeted data and had collected wireless signals from those devices over a long period of time (both challenging criteria in themselves), it would require significant resources to use a quantum computer to derive 128-bit symmetric keys from each of those devices (Mitchell, 2020).

Priority for Assistance
We rated the NCF as a medium priority for assistance. The high overall ratings in the assessed categories are nevertheless significantly mitigated by the practical difficulty that would be involved with carrying out an attack that would meaningfully degrade or disrupt the function.

References
Works That Informed the Analysis
CISA, National Security Agency; and Office of the Director of National Intelligence, “Potential Threat Vectors to 5G Infrastructure,” 2021.
FactSet, financial data and analytics, 2021.
National Critical Function 9, Provide Wireline Access Network Services

Category: Connect

Summary

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>High Certificate authorities, hardware manufacturers, network operators, and other organizations all likely need to address vulnerabilities.</td>
</tr>
<tr>
<td>Cost</td>
<td>High Updates will likely include large-scale deployments of new software or certificates to devices and industrywide hardware development and procurement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating The national critical function (NCF) has strong organizational support, and these organizations have been proactive in developing solutions to the issues affecting the NCF.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium Despite mitigating factors, the expected scope and cost of updates lead to a rating of medium priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Network providers must adopt post-quantum cryptography (PQC) to secure network access. A significant amount of hardware is likely to be affected, and costs for updates could be substantial.</td>
</tr>
</tbody>
</table>

CISA definition: "Operate circuit- and packet-switched networks via copper, fiber, and coaxial transport media, including private enterprise data and telephony networks and the public switched telephone network (PSTN)" (CISA, 2020b, p. 3).

Synopsis of Issues

This NCF covers long-haul transport networks, metropolitan fiber networks, and the last mile of wired network access (Working Group 4, 2015), and many of the affected organizations and systems are the same as those in NCF 2, Provide Cable Access Network Services. The assessment and context for this NCF are therefore largely identical to those for NCF 2.

The NCF has a role in the transmission of encrypted voice, video, and data traffic across wired networks. If sensitive data are transmitted over a wired network, the sender and receiver endpoints, not the network operators are those with the primary responsibility for the encryption operations on those data. Wired network operators also often encrypt traffic flows between individual modems and an operator’s terminal network system to prevent a network user from reading traffic that was not already encrypted (CableLabs, 2017). That encryption is not a significant vulnerability with respect to quantum computing, however, because it uses symmetric-key cryptography. In its own operations, the NCF also does not use or control data with a long confidentiality lifetime, so it presents no clear catch-and-exploit vulnerabilities.

The NCF will experience significant authentication vulnerabilities in its operations due to extensive use of vulnerable public-key infrastructures, as dictated by industrywide specifications, especially Data over Cable Service Interface Specifications (DOCSIS). The industry uses a chain of digital certificates to identify cable modems at endpoints (e.g., users, content providers, operator hardware) and control access to the network for those modems. At production time, modems have certificates for the device and the manufacturer installed. Other certificates are used to validate software and firmware updates to modems and routing hardware (Van Deynse, 2015). An attacker with a quantum computer could exploit the vulnerability in these certificates at multiple points in this chain (root certificate authority, trusted manufacturer, operator, or device), unless these certificates are replaced with quantum-resistant versions. This would allow the attacker to gain access to devices and operator networks or install software onto a network. Finally, vulnerabilities in public-key
Preparing for Post-Quantum Critical Infrastructure

infrastructure used to secure routing messages using the border gateway protocol would also present vulnerabilities for this NCF, although this is a more relevant issue for NCF 4, Provide Internet Routing, Access, and Connection Services.

Urgency
Our assessment is that urgency of action for this NCF is low. No catch-and-exploit issues are apparent, and it is unlikely any of the authentication vulnerabilities will be extensive or challenging enough to necessitate urgent attention. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap. The most significant authentication vulnerabilities are those that would allow an attacker to impersonate a root certificate authority or trusted manufacturer to control hardware or perform widespread dissemination of malicious software. Those organizations must transition to certificates that use PQC only before a quantum computer arrives. Although vulnerable cryptographic systems are typically embedded in hardware at production and that hardware can be in use for long durations (i.e., 20 or more years), mechanisms exist for gradually addressing those vulnerabilities after deployment (Pala, 2020; Van Deynse, 2015).

Scope
Our assessment is that scope for this NCF is high. Standard-setting bodies, certificate authorities, hardware manufacturers, and network operators are all likely to require varying degrees of active engagement to address quantum computing vulnerabilities.

Cost
Our assessment is that cost per organization for this NCF is high. Many mitigation actions are likely to be straightforward, centralized actions that are massive in scope. For example, certificate authorities might need to deploy and sign hundreds of millions of new certificates, or operators and manufacturers might need to employ multiple strategies to remotely deploy upgrades to different classes of fielded devices while ensuring backward compatibility (Pala, 2020; Van Deynse, 2015). Other mitigation actions will require hardware work-arounds or redesigns that will need to be developed and tested according to newly developed specifications. Where work-arounds are inadequate and PQC deployment creates performance bottlenecks, new hardware might need to be acquired (Pala, 2021).

Other Factors
Our assessment is that other factors for this NCF are mitigating. The industry is aware of the vulnerabilities from quantum computing and proactively working to address them. Documented activities include planned updates to industrywide specifications, such as DOCSIS, creation of new cryptographic libraries, and ongoing investigation of the operational challenges that PQC might create (Pala, 2020; Pala, 2021; Stebila and Mosca, 2017). The NCF as a whole is well supported by government and industry organizations, such as CableLabs, Excentis, the Open Connectivity Foundation, the Broadband Internet Technical Advisory Group, and the Communications Security, Reliability, and Interoperability Council of the Federal Communications Commission. Finally, the distributed, redundant nature of connections between cable networks is likely to make them resilient to a broader disruption from attacks on single network providers, similar to other network access NCFs (e.g., NCF 4, Provide Internet Routing, Access, and Connection Services) (DHS, 2009).

Priority for Assistance
We rated the NCF as a medium priority for assistance. Organizations in this NCF likely have the industry support needed to understand the problems affecting them and the solutions to those problems. The cost for
implementing those solutions is likely to be substantial, however, and the scope of affected organizations is broad.

References

Works That Informed the Analysis
Van Deynse, David, “Certificates and Different PKIs in DOCSIS 3.1,” Excentis, July 17, 2015.

Related Reading
National Critical Function 10, Distribute Electricity

Category: Distribute

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Updates need to happen only before a cryptographically relevant quantum computer (CRQC) is available, but forward compatibility with post-quantum cryptography (PQC) should be incorporated into existing modernization efforts to avoid embedding vulnerability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
<td>Thousands of providers in this national critical function (NCF) will need to address updates of varying kinds.</td>
</tr>
<tr>
<td>Cost</td>
<td>High</td>
<td>The operational complexity and heterogeneity of systems and regulations across the United States will lead to high costs because each system independently assesses where and how to incorporate PQC.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>The heterogeneity of the NCF could slow adoption of PQC, but ongoing modernization efforts and redundant security in industrial control system (ICS) networks might mitigate cost and urgency.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>High</td>
<td>The NCF is a high priority for assistance, despite medium urgency, because of the broad, heterogeneous scope and high expected costs.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap, with an emphasis on ensuring forward compatibility with PQC in ongoing modernization efforts.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Maintain and operate medium- to low-voltage system to reliably supply consumer demand for electricity from the bulk electric power network” (CISA, 2020b, p. 3).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

The NCF will experience authentication vulnerabilities in information technology (IT) systems and cyber-physical systems. The NCF consists of a diverse group of stakeholders, owners, and operators that use a complex mix of aging and modern communication, control, and distribution systems (Smart Grid Cybersecurity Committee, 2014). Internet-based communication systems and public-key infrastructures are increasingly used to improve interoperability and cybersecurity (Kuzlu, Pipattanasomporn, and Rahman, 2014), and these will present quantum computing vulnerabilities in authentication where they are used. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.1

---

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and con-
Urgency
Our assessment is that urgency of action for this NCF is medium. The NCF is in the midst of a significant modernization effort, and new software and hardware systems are being implemented to improve automation (Smart Grid Cybersecurity Committee, 2014; Marston, 2018). Although systems need to complete a migration to PQC only before a CRQC, it will nevertheless be important that the NCF address the migration to PQC with some urgency. Any systems being modernized now without addressing forward compatibility with a PQC standard could embed long-lived vulnerability into systems that might be challenging or costly to update in the future, increasing the likelihood that significant vulnerabilities remain after the arrival of a CRQC. Organizations should begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is high. More than 3,000 providers sell power to customers in the United States (Marston, 2018), and a significant portion of them might need to take action of some kind.

Cost
Our assessment is that cost per organization for this NCF is high. The operational complexity of electricity distribution and the heterogeneity of the function across the United States will make it challenging to find easily standardized solutions. Distribution often requires communication between multiple different kinds of communication and distribution technologies, and real-time monitoring and control are critical to operations (Kuzlu, Pipattanasomporn, and Rahman, 2014). Incorporating PQC (and potentially stronger keys in ICSs, in which symmetric keys and hashing are used for security) could introduce additional latency in communications and additional complexity to communication and distribution management systems, and this could lead to significant cost for each affected organization as it addresses how PQC migration uniquely affects its operations.

Other Factors
Our assessment is that other factors for this NCF are neutral on balance, with exacerbating and mitigating factors identified. In contrast to NCF 12, Transmit Electricity, which is governed by significant federal regulatory authority, regulatory responsibilities for distribution systems are the purview of state regulators—distribution systems do not have federal oversight for reliability (Marston, 2018; Warwick et al., 2016). The heterogeneity of distribution systems and regulatory authority across the United States might present a further challenge to interoperability with systems that migrate to PQC, which could slow the broader migration across the NCF. We assessed this as a significant exacerbating factor.

The NCF is already facing substantial costs as it makes widespread updates to software and hardware to enable greater automation in electricity distribution (Marston, 2018). This ongoing modernization effort presents an opportunity to incorporate quantum-resistant solutions in distribution infrastructure, provided that the hardware and software solutions supplied by other NCFs begin to include compatibility with PQC by default. Although, in many cases, implementing quantum-resistant solutions could increase operational

...
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

complexity (and therefore increase cost, as discussed earlier), in others, migration costs might be decreased by modernization efforts. That is, because operators are already updating systems to improve the function, interoperability, and reliability of the distribution system, there is a greater likelihood that many updated systems could incorporate PQC by default without additional effort or cost incurred by the operators. We assessed this as a mitigating factor.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant network security mechanisms that would further mitigate vulnerability, even where long-lived operational technologies were deployed with vulnerable cryptographic security mechanisms (ICS-CERT, 2016). This presents a mitigating factor.

Priority for Assistance

We rated the NCF as a high priority for assistance. Many organizations in the NCF are affected, and electricity distribution has a high degree of operational complexity. The NCF is undergoing a significant modernization effort, and it will be important that the NCF be aware of the vulnerabilities from quantum computing so that forward compatibility with PQC can be incorporated in these ongoing efforts. The heterogeneity of distribution systems and regulation across the United States could also make widely standardized solutions challenging, and operators could face significant costs from addressing quantum computing vulnerabilities.

References

Works That Informed the Analysis


Related Reading
National Critical Function 11, Maintain Supply Chains

Category: Distribute

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td></td>
</tr>
<tr>
<td>Scope</td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td></td>
</tr>
<tr>
<td>Other factors</td>
<td></td>
</tr>
<tr>
<td>Priority for assistance</td>
<td></td>
</tr>
</tbody>
</table>

Updates to relevant products and services from other national critical functions (NCFs) can happen gradually, provided that they are complete when a capable quantum computer arrives.

Issues will be addressed largely by other NCFs. Situations requiring active, swift risk mitigation are likely to be rare.

Mitigation is likely to take place through software updates and in-cycle hardware replacement.

We identified no other relevant mitigating or exacerbating factors.

Low ratings in all categories lead to a rating of low priority for assistance.

This NCF will rely on other NCF dependencies to address authentication vulnerabilities in its products and services in a timely manner. Organizations in this NCF should begin early preparations for the post-quantum cryptography (PQC) migration following the U.S. Department of Homeland Security (DHS) roadmap, especially with respect to creating an inventory of public-key cryptography uses in supply chains.

CISA definition: “Manage and sustain the networks of assets, systems, and relationships that enable the movement of goods and services from producers to consumers” (CISA, 2020b, p. 3).

Synopsis of Issues

We did not identify any specific quantum computing vulnerabilities directly affecting this NCF that were not more appropriately discussed in depth in assessments for other NCFs. This NCF is indirectly affected by quantum computing vulnerabilities in public-key encryption used in many other NCFs that are critical to the maintenance of supply chains.

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

This NCF will experience authentication vulnerabilities in products and services provided by other NCFs, and it will be dependent on those NCFs addressing those vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. Other NCFs (especially Distribute NCFs, such as NCFs 13 to 17) are also likely critical dependencies for this NCF, but they will similarly be dependent on NCFs 3 and 52 to address vulnerabilities. The use of networked enterprise information technology products (e.g., software and services for network connectivity, enterprise resource planning, supply chain management, knowledge management) is critical to the maintenance of supply chains, and quantum computing vulnerabilities affecting this NCF arise primarily from the use of public-key cryptography in those products and services. These NCFs will need to address authentication vulnerabilities in products and services provided to this NCF before a cryptographically relevant quantum computer arrives.

Urgency

Our assessment is that urgency of action for this NCF is low. Networked enterprise information technology products and services will need to be updated and, in some cases, built over time through software updates,
Preparing for Post-Quantum Critical Infrastructure

security patches, and hardware replacements, but systems need complete updates only prior to the arrival of a cryptographically relevant quantum computer. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
We identified no other relevant mitigating or exacerbating factors for this NCF.

Priority for Assistance
We rated the NCF as a low priority for assistance. We gave low ratings in all assessed factors, largely because relevant issues should be addressed in products and services provided by other NCFs.

References
Works That Informed the Analysis
National Critical Function 12, Transmit Electricity

Category: Distribute

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
<td>Regional transmission operators, independent system operators, all electric utilities, certificate authorities, hardware manufacturers, network operators, and other organizations all likely need to address vulnerabilities.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Although, industrywide, the cost might be significant and some organizations might be exceptions that incur high costs, the overall cost per organization is likely to be low across the national critical function (NCF). New certificates will need to be issued, but other updates can take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>The regulated nature of the NCF can give supporting organizations leverage to drive the migration to post-quantum cryptography (PQC) across the NCF.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low urgency, low cost, and the regulated nature of the NCF lead to a rating of low priority, despite the high scope.</td>
</tr>
</tbody>
</table>

Primary concern(s)

- PQC should be incorporated into industrywide communication standards, such as those from the Open Access Same-Time Information System (OASIS).
- Organizational network access and systems that secure industrial control systems (ICSs) must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Maintain and operate high-voltage (>100 kV [kilovolt]) bulk electric system to reliably supply distribution network demand for electricity from generation resources” (CISA, 2020b, p. 3).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

The NCF will experience authentication vulnerabilities in information technology (IT) systems, cyber-physical systems, and industry-specific communication systems. Organizations in the NCF are required under federal regulations to “comply with the business practice and electronic communication standards promulgated by the North American Energy Standards Board (NAESB) Wholesale Electric Quadrant (WEQ)” (18 C.F.R. Parts 37–38). WEQ standards promulgated by NAESB dictate the use of OASIS, an Internet-based system that depends on public-key infrastructures (PKIs) to facilitate a variety of authenticated actions, including financial transactions, transmission scheduling, and communication and data transfers (WEQ, undated; WEQ, 2009). The use of a PKI makes this system an important authentication vulnerability for the NCF. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and
services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.¹

**Urgency**

Our assessment is that urgency of action for this NCF is low. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and in-cycle hardware replacements. Post-quantum PKI will need to be instituted, but a system need complete these changes only prior to the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is high. The centralized regulatory and standard-setting bodies for the NCF will need to address the incorporation of PQC into communication standards for the NCF. Nationally, high-voltage transmission services connect approximately 7,000 power plants to the power grid (Office of Electricity Delivery and Energy Reliability, 2015). Regional transmission operators, independent system operators, electric utilities, and many other organizations that are authorized to access applications secured under the WEQ PKI standards (as defined in WEQ, 2009) will need to take individual action of some kind to use the new PKI standard.

**Cost**

Our assessment is that cost per organization for this NCF is low overall, but some notable exceptions might incur higher costs. Most participants authorized to access applications using the WEQ PKI standard will incur low costs because they will likely need only to have digital certificates reissued (likely accompanied by a fee) and might need to address other configuration changes or vendor-provided software updates for IT and ICSs. The regulatory and standard-setting bodies will need to develop a new standard and certification program that incorporates PQC in the PKI standard and test the impact on the industry. This could incur a high cost. Organizations that provide certificate authority or registration authority services for the industry PKI could incur high costs from all activities associated with the reissuance of thousands of certificates that are compliant with the new standard. Any ICSs currently using public-key cryptography for authenticated access and control will need to eventually be updated as well. Organizations should begin to follow the preparation steps outlined in the DHS roadmap.

**Other Factors**

Our assessment is that other factors for this NCF are mitigating. The electric power grid is operationally complex and managed and supported by a diverse ecosystem of organizations. Despite that complexity, however, this NCF is highly regulated and supported by authoritative policies on cybersecurity standards and practices. These standards are cooperatively developed and advanced by the Federal Energy Regulatory Commis-

---

¹ This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, PKIs and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

sion, NAESB, North American Electric Reliability Corporation, and other regional partners. The regulatory authority to enforce standards and certification gives significant leverage to drive the migration to PQC. This will increase the likelihood that the NCF can migrate to PQC before a CRQC arrives, and it presents a strong mitigating factor.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant network security mechanisms that would further mitigate vulnerability, even where long-lived operational technologies were deployed with vulnerable cryptographic security mechanisms (ICS-CERT, 2016). This presents a further mitigating factor.

Priority for Assistance

We rated the NCF as a low priority for assistance. Many organizations in the NCF are affected, and the electric grid has a high degree of operational complexity, but urgency is low, and most organizations will not face high costs from the migration to PQC. Moreover, the regulation of the industry will be beneficial in driving the adoption of new standards across the industry.

References

Works That Informed the Analysis


———, Public Key Infrastructure (PKI), Standard WEQ-012, version 002.1, March 11, 2009.


Related Reading


National Critical Function 13, Transport Cargo and Passengers by Air

Category: Distribute

Summary

| Urgency | Medium | This national critical function (NCF) regularly handles personally identifiable information (PII) and proprietary business information with a moderate confidentiality lifetime. Communications that do not create catch-and-exploit vulnerabilities need to adopt post-quantum cryptography (PQC) only before a cryptographically relevant quantum computer arrives, but hardware can have a long lifetime in the field and needs to integrate forward compatibility with PQC soon. |
| Scope   | Medium | Vendors and manufacturers of aviation communication equipment will be affected. |
| Cost    | Medium | Vendors and manufacturers will need to design to a modified specification, which might involve limited software development or hardware redesigns. |
| Other factors | Mitigating | The NCF has strong public and private institutional support and multiple ongoing cybersecurity initiatives, and it has tested PQC in aviation communications. |
| Priority for assistance | Medium | Medium ratings in all categories lead to a medium priority for assistance. |
| Primary concern(s) |  | Bodies governing communication standards for civil aviation need to incorporate PQC into communication standards and equipment specifications so equipment manufacturers can begin to design in forward compatibility with the updated standard. |

CISA definition: “Provide and operate aviation systems, assets, and facilities to enable a system of securely and safely conveying goods and people from place to place by air” (CISA, 2020b, p. 3).

Synopsis of Issues

This NCF does handle some information in transit with a moderate confidentiality lifetime, including passenger PII and proprietary business information. These data would generally have a short to medium confidentiality lifetime, and they will exhibit catch-and-exploit vulnerabilities until PQC is used in key exchange to secure data in transit.

The NCF will exhibit authentication vulnerabilities in the systems used by civil air travel organizations to facilitate networked telecommunications between aircraft and multiple terrestrial and satellite communication networks. These vulnerabilities arise from the extensive use of public-key infrastructures (PKIs) to identify and authenticate entities across the many networks involved in civil air travel (Ben Mahmoud, Pirovano, and Larrieu, 2014; Byrne, 2018; Federal Aviation Administration, 2020a; Federal Aviation Administration, 2020b; Mäurer and Bilzhouse, 2018). The PKIs currently used by the NCF rely on public-key cryptography methods that will be vulnerable to an attacker with a capable quantum computer. The NCF will need to transition to post-quantum algorithms for certificates, signatures, and key exchange in each of these NCF-specific networks and systems before a capable quantum computer arrives. Failing to do so would result in an attacker being able to intercept or fake secure aviation communications. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in software products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management).
Urgency
Our assessment is that urgency of action for this NCF is medium. Operators in the NCF will handle passenger PII and commercial logistics and financial information that might constitute proprietary business information. Like in other NCFs responsible for protecting PII (except protected health information [PHI]) and proprietary business information, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years) and their protection from catch and exploit justifies an assessment of medium urgency. Authentication issues will require the migration to PQC in PKIs used by networked systems in civil aviation, but this must be done only before a quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security roadmap. Much of the communication equipment is installed in other long-lived equipment, such as facilities, vehicles, and aircraft, and could have a long lifetime in the field. For that reason, it is important that communication devices begin to be designed to be forward compatible with the use of PQC in aviation communication standards as soon as practical to avoid the need for widespread, costly hardware replacements in the future.

Scope
Our assessment is that scope for this NCF is medium. A small number of central organizations act as coordinating bodies for the communication standards and network architectures used in civil aviation. Standards governing network architectures, such as the Aeronautical Mobile Airport Communication System, and L-Band Digital Aeronautical Communications System, and any other PKI-dependent communication protocol used in civil aviation will need to incorporate a new standard for post-quantum PKI into their own certification scheme. After this integration has occurred, each vendor or manufacturer of a product built to the specifications of those communication standards will need to take action to enable the use of the post-quantum standard in that product. We estimate that the number of affected organizations would be between ten and 100 (FactSet, 2021). Organizations using these products and services should be able to effect the change with routine software updates and in-cycle hardware refreshes, provided that vendors and manufacturers begin to design in forward compatibility with PQC soon. Implementing organizations (e.g., airports) are therefore not included in scope.

Cost
Our assessment is that cost per organization for this NCF is medium. Once new communication standards incorporating PQC are defined, vendors and manufacturers of products built to the specifications and performance requirements of those standards will need to update their products to enable the use of PQC algorithms. The new specifications could involve changes to cryptographic key length or message sizes, and the product changes could require limited software development or hardware redesigns.

Other Factors
Our assessment is that other factors for this NCF are mitigating. The aviation industry has a strong foundation of public and private institutional support, including such organizations as the Federal Aviation Administration, the International Civil Aviation Organization, the International Air Transport Association, and the Worldwide Interoperability for Microwave Access Forum. Collectively, these groups have the prerogative to set standards, specifications, and certification schemes for the industry then mandate their use. Multiple industry network security initiatives are ongoing (Ben Mahmoud, Pirovano, and Larrieu, 2014), and the civil aviation industry is already testing the use of PQC algorithms for communication within existing communication standards (Mielke et al., 2021). Supporting institutions emphasizing the importance of PQC in future
communication standards and planning for the migration would provide a significant mitigating factor for
the NCF.

**Priority for Assistance**

We rated the NCF as a medium priority for assistance because it had medium ratings in each category. The
NCF also has significant institutional support and has publicly documented efforts to test PQC algorithms
in existing communication standards.

**References**

**Works That Informed the Analysis**

Ben Mahmoud, Mohamed Slim, Alain Pirovano, and Nicolas Larrieu, “Aeronautical Communication Transition
pp. 1–29.

Byrne, Declan, “AeroMACS at a Glance: Moving Towards the Airport 3.0,” Worldwide Interoperability for


FactSet, financial data and analytics, 2021.


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.

Mielke, Daniel M., Nils Mäurer, Thomas Gräupl, and Miguel Bellido-Manganell, “Getting Civil Aviation Ready


**Related Reading**

2016.
National Critical Function 14, Transport Cargo and Passengers by Rail

Category: Distribute

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>This national critical function (NCF) regularly handles personally identifiable information (PII) and proprietary business information with a moderate confidentiality lifetime. Other updates to address authentication vulnerabilities can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issues will be addressed largely by other NCFs. Situations requiring active, swift risk mitigation are likely to be rare.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cost</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other factors</th>
<th>Mitigating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems. The NCF also has effective organizational support from industry groups.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Priority for assistance</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low ratings in most categories lead to a rating of low priority for assistance.</td>
<td></td>
</tr>
</tbody>
</table>

| Primary concern(s) | Organizational network access and systems that secure ICSs must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap. |

CISA definition: “Provide and operate freight and passenger railroad systems, including conveyances, infrastructure, and management systems to enable a system of securely and safely conveying goods and people from place to place by rail” (CISA, 2020b, p. 3).

Synopsis of Issues

This NCF does handle some information in transit with a moderate confidentiality lifetime, including passenger PII and proprietary business information. These data would generally have a short to medium confidentiality lifetime, and they will exhibit catch-and-exploit vulnerabilities until PQC is used in key exchange to secure data in transit.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology (IT) products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.1

---

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 43, 44, 45, 46, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastruc-
Urgency
Our assessment is that urgency of action for this NCF is medium. Operators in the NCF will handle passenger PII and commercial logistics and financial information that could constitute proprietary business information. Like in other NCFs responsible for protecting PII (except protected health information [PHI]) and proprietary business information, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years), and their protection from catch and exploit justifies an assessment of medium urgency. Cyber-physical systems and network account access will also need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs. As a result, appropriate actions (e.g., configuring commercial products to use PQC in key exchange) from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. Deployed ICS technology is often resource-constrained, and industries often opt to use less vulnerable cryptographic security mechanisms (e.g., pre-shared symmetric keys or hashing algorithms) in some operational technology because they require fewer computational resources (Stouffer et al., 2015). Networked ICSs often also rely on additional, redundant network security mechanisms that would further mitigate vulnerability, even where long-lived operational technologies were deployed with vulnerable cryptographic security mechanisms (ICS-CERT, 2016).

The NCF is effectively supported by federal agencies and industry groups, such as the Rail Information Security Committee and the Association of American Railroads (Association of American Railroads, 2021). A recent report on cybersecurity issues affecting the industry specifically mentions the importance of cryptographic system management in cybersecurity management (Rail Information Security Committee, 2018). The industry will likely have all the information and resources needed to transition on an appropriate timescale once standards and updated IT products and services are available.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in most assessed factors.

References
Stouffer et al., 2015. Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
References

Works That Informed the Analysis


National Critical Function 15, Transport Cargo and Passengers by Road

Category: Distribute

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
</tr>
</thead>
</table>

This national critical function (NCF) regularly handles personally identifiable information (PII) and proprietary business information with a moderate confidentiality lifetime. Other communications in connected roadside infrastructure must adopt post-quantum cryptography (PQC) only before a quantum computer arrives.

<table>
<thead>
<tr>
<th>Scope</th>
<th>Low</th>
</tr>
</thead>
</table>

A few centralized bodies coordinating standardization must address the incorporation of PQC into existing efforts.

<table>
<thead>
<tr>
<th>Cost</th>
<th>Low</th>
</tr>
</thead>
</table>

PQC migration can be incorporated into existing system engineering approaches to the standards for connected roadside infrastructure.

<table>
<thead>
<tr>
<th>Other factors</th>
<th>Mitigating</th>
</tr>
</thead>
</table>

The NCF has strong institutional support from regulatory and standard-setting organizations, and research on the use of PQC in vehicle communications already exists.

<table>
<thead>
<tr>
<th>Priority for assistance</th>
<th>Low</th>
</tr>
</thead>
</table>

Low ratings in most categories lead to a rating of low priority for assistance.

| Primary concern(s) | Ongoing standardization activities for connected roadside infrastructure should incorporate plans for using PQC in vehicle-to-vehicle and vehicle-to-infrastructure communication standards and specifications. |

CISA definition: “Provide and operate roadway systems, assets, and facilities—including commercial motor carriers and associated facilities, motor coaches, buses, and associated systems, assets, and facilities—to enable a system of securely and safely conveying goods and people from place to place by highway” (CISA, 2020b, p. 3).

Synopsis of Issues

This NCF does handle some information in transit with a moderate confidentiality lifetime, including passenger PII and proprietary business information. These data would generally have a short to medium confidentiality lifetime, and they will exhibit catch-and-exploit vulnerabilities until PQC is used in key exchange to secure data in transit.

The NCF will experience authentication vulnerabilities in the systems used to facilitate communication between connected road vehicles, connected roadside infrastructure, and the broader Internet. Intelligent transportation systems (ITSs), the ecosystem of connected road infrastructure and vehicles, utilize public-key infrastructures to identify connected entities and determine their data access and control permissions (Hasan et al., 2020). These public-key infrastructures currently use vulnerable public-key encryption algorithms, and they would allow an attacker with a capable quantum computer to gain access to any connected roadside infrastructure or vehicle until those systems adopt PQC. These systems must all migrate to PQC before a capable quantum computer arrives.

Urgency

Our assessment is that urgency of action for this NCF is medium. Operators in the NCF will handle passenger PII and commercial logistics and financial information that could constitute proprietary business information. Like in other NCFs responsible for protecting PII (except protected health information [PHI]) and proprietary business information, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years), and their protection from catch and exploit justifies an assessment of medium urgency. Authentication issues must be addressed only before a quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security roadmap. Many of the concepts and technologies that will be used to facilitate a...
connected roadside environment are still in pilot phases, so the migration to PQC in these systems can coincide with that broader development, testing, and deployment (ITS Joint Program Office, undated b).

Scope
Our assessment is that scope for this NCF is low. The scope includes the organizations and consortia involved in setting standards and performing testing for ITSs. Although these standard-setting activities have many stakeholders, they are coordinated and harmonized by just a few organizations, such as the U.S. Department of Transportation ITS Joint Program Office (ITS Joint Program Office, undated a).

Cost
Our assessment is that cost per organization for this NCF is low. Standards governing ITSs are still in development and testing. The relative technological immaturity of the ITS ecosystem might allow for PQC to be incorporated into the ongoing system engineering approach to standard development and harmonization without the significant costs that would otherwise be incurred in more-mature, complex technology ecosystems. Although using PQC especially in vehicle-to-vehicle and vehicle-to-infrastructure communication could create challenges (Bindel, McCarthy, et al., 2021), these can be addressed as part of ongoing system engineering for related standards and technology.

Other Factors
Our assessment is that other factors for this NCF are mitigating. The NCF has strong institutional support from organizations in the U.S. Department of Transportation, consortia of companies in the commercial sector, and international partners. Some organizations are already managing communication standardization activities and technology test beds (ITS Joint Program Office, undated b), and research efforts are examining issues related to the use of PQC in ITSs (Bindel, McCarthy, et al., 2021).

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in most categories and evidence that organizations in the NCF are already engaged in addressing the use of PQC in connected roadside technologies.

References
Works That Informed the Analysis


National Critical Function 16, Transport Cargo and Passengers by Vessel

Category: Distribute

Summary

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Medium</td>
<td>This national critical function (NCF) regularly handles personally identifiable information (PII) and proprietary business information with a moderate confidentiality lifetime. Other updates to address authentication vulnerabilities can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely in products and services provided by other NCFs. Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in most categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Network access and cyber-physical system controls in ashore and shipboard operations must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Provide and operate maritime systems, assets, and facilities to enable a system of securely and safely conveying goods and people from place to place by the Maritime Transportation System” (CISA, 2020b, p. 4).

Synopsis of Issues

This NCF does handle some information in transit with a moderate confidentiality lifetime, including passenger PII and proprietary business information. These data would generally have short to medium confidentiality lifetimes, and they will exhibit catch-and-exploit vulnerabilities until PQC is used in key exchange to secure data in transit.

The NCF will exhibit authentication vulnerabilities from the increasing use of public-key infrastructures (PKIs) in shipboard and ashore operations. Like in many other NCFs, authentication vulnerabilities will be present in networked business information technology (IT) products and services used in ashore operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components in ports (e.g., ICS or supervisory control and data acquisition [SCADA] systems, cranes, sensors, and programmable logic controllers). Card-based access control mechanisms, such as the Transportation Worker Identification Credential, depend on vulnerable PKIs as part of the authentication mechanism (Chandramouli, 2014). Shipboard operations are also increasingly digitized and able to connect to Internet-based services, and the industry is moving toward greater use of PKI for authenticated communications (Bour et al., 2020). Any PKI-dependent shipboard IT system or cyber-physical system will be similarly vulnerable. These authentication vulnerabilities are primarily in software products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based
Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services).\(^1\)

**Urgency**

Our assessment is that urgency of action for this NCF is medium. Operators in the NCF will handle passenger PII and commercial logistics and financial information that could constitute proprietary business information. Like in other NCFs responsible for protecting PII (except protected health information [PHI]) and proprietary business information, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years), and their protection from catch-and-exploit justifies an assessment of medium urgency. Cyber-physical systems and network account access will also need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs. As a result, appropriate actions (e.g., configuring commercial products to use PQC in key exchange) from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are mitigating. Deployed ICS technology is often resource-constrained, and industries often opt to use less vulnerable cryptographic security mechanisms (e.g., pre-shared symmetric keys or hashing algorithms) in some operational technology because they require fewer computational resources (Stouffer et al., 2015). Networked ICSs often also rely on additional, redundant network security mechanisms that would further mitigate vulnerability, even where long-lived operational technologies were deployed with vulnerable cryptographic security mechanisms (ICS-CERT, 2016).

**Priority for Assistance**

We rated the NCF as a low priority for assistance because of its low ratings in most categories.

---

\(^1\) This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, PKIs and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
References

Works That Informed the Analysis


# National Critical Function 17, Transport Materials by Pipeline

**Category:** Distribute

## Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Urgency</th>
<th>Scope</th>
<th>Cost</th>
<th>Other factors</th>
<th>Priority for assistance</th>
<th>Primary concern(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Exacerbating</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>

Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.

Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.

Mitigation is likely to take place through software updates and in-cycle hardware replacement.

The NCF is operationally complex, has historically not prioritized cybersecurity, and lacks a common approach to standardization and cybersecurity. Layered security in industrial control system (ICS) networks could mitigate some vulnerability in connected cyber-physical systems.

Low ratings in all categories lead to a rating of low priority for assistance.

Organizational network access and systems that secure ICSs must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

### CISA definition:

"Provide and operate systems, assets, and facilities to enable a system of securely and safely conveying materials from place to place by pipelines" (CISA, 2020b, p. 4).

## Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

The NCF will experience authentication vulnerabilities in information technology (IT) systems and cyber-physical systems. The NCF consists of a diverse group of stakeholders, owners, and operators that use a complex mix of aging and modern communication, control, and distribution systems (Nygaard and Mukhopadhyay, 2020). Internet-based communication systems are increasingly used to improve interoperability and cybersecurity (Stouffer et al., 2015), and these will present quantum computing vulnerabilities in authentication where they are used. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of

---

1. The oil and natural gas supply chain (described in Nygaard and Mukhopadhyay, 2020) integrates elements from NCF 17, Transport Materials by Pipeline; 41, Store Fuel and Maintain Reserves; 43, Exploration and Extraction of Fuels; and 44, Fuel Refining and Processing Fuels. As a result, the assessments for the NCFs address many of the same organizations, IT and operational technology systems, and vulnerabilities, and their content is very similar.
these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.²

Urgency
Our assessment is that urgency of action for this NCF is low. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and in-cycle hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Although the oil and natural gas (ONG) industry alone includes thousands of organizations and stakeholders (FactSet, 2021), most will not need to take significant action that specifically addresses quantum computing vulnerabilities, and they are therefore not included in the scope. Each stakeholder will need to consider how quantum computing vulnerabilities need to be integrated into broader cybersecurity risk management and associated IT and operational technology acquisition strategy. Most affected products and services are provided by other NCFs, however, and those NCFs will likely provide many of the required updates.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. Mitigation is likely to take place through configuration changes, software updates, security patches, and in-cycle hardware replacement for affected technologies. Where vulnerabilities remain that are not addressed by those actions, the industry’s ongoing adoption of defense-in-depth strategies in ICS is likely to be adequate for risk reduction related to quantum computing (ONG Subsector Coordinating Council, 2018).

Other Factors
Our assessment is that other factors for this NCF are exacerbating on balance, with mitigating and exacerbating factors present. The ONG industry increasingly integrates legacy operational technology and IT with modern automated, connected systems in order to improve productivity, but the industry as a whole has generally not adequately prioritized cybersecurity. Moreover, the industry has not exhibited effective coordination with federal partners on cybersecurity (especially ICS security) incident prevention and management, although this has been improving in recent years. Regulation and standardization in the industry are also complex:

[T]he sheer number of differing regulatory bodies and trade groups offering both standards and best-practice recommendations for ONG cyber-security makes it difficult to create a comprehensive, directed,

² This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
and coherent strategy that is applicable to all players within the ONG industry. (Nygaard and Mukhopadyay, 2020, p. iii)

Together, these factors indicate a strong possibility that the NCF will not respond to risks from quantum computing vulnerabilities in a robust, coordinated, and timely manner, and we assessed this to be a significant exacerbating factor.

Deployed ICS technology is often resource-constrained, and 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). Networked ICSs often also rely on additional, redundant 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; ONG Subsector Coordinating Council, 2018). We assessed this as a mitigating factor.

**Priority for Assistance**
We rated the NCF as a low priority for assistance because of its low ratings in most assessed factors.

**References**

*Works That Informed the Analysis*
FactSet, financial data and analytics, 2021.
National Critical Function 18, Transport Passengers by Mass Transit

Category: Distribute

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>This national critical function (NCF) regularly handles personally identifiable information (PII) with a moderate confidentiality lifetime. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely in products and services provided by other NCFs. Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in most categories lead to a rating of low priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td></td>
<td>Organizational network access and systems that secure ICSs must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
</tr>
</tbody>
</table>

CISA definition: “Provide and operate systems, assets, and facilities to enable a system of securely and safely conveying people from place to place by roads or on fixed guideways within a specified geographic area—including transit buses, trolleybuses, monorails, heavy rail (subway), light rail, passenger rail, commuter rail, and vanpool/rideshare” (CISA, 2020b, p. 4).

Synopsis of Issues

This NCF does handle some information in transit with a moderate confidentiality lifetime, including passenger PII. These data would generally have a short to medium confidentiality lifetime, and they will exhibit catch-and-exploit vulnerabilities until PQC is used in key exchange to secure data in transit.

Like in many other NCFs, this NCF will experience authentication vulnerabilities in networked enterprise information systems (e.g., software for enterprise resource management or customer relationship management and cloud-based services) and connected cyber-physical systems used in operations (e.g., ICS or supervisory control and data acquisition [SCADA] used to control or monitor transportation equipment). According to the American Public Transportation Association, these systems are often “interrelated into multimodal systems such as buses, ferries and metro modes” (American Public Transportation Association, 2014, p. 3). In most cases, these systems will be dependent on vulnerable public-key cryptography–based authentication mechanisms (e.g., public-key infrastructures or virtual private networks [VPNs]) to facilitate secure communications and operations between networked systems. These authentication vulnerabilities are primarily in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Each system will need to migrate to PQC for authentication before a CRQC arrives.1

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business information technology systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for
Urgency
Our assessment is that urgency of action for this NCF is medium. Operators in the NCF will handle PII and proprietary business information with a moderate confidentiality lifetime. Like other NCFs responsible for protecting PII (except protected health information [PHI]) and proprietary business information, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years), and their protection from catch and exploit justifies an assessment of medium urgency. Internet-dependent IT products and services, including remote access to critical databases, will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs. As a result, appropriate actions (e.g., configuring commercial products to use PQC in key exchange) from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. Deployed ICS technology is often resource-constrained, and industries often opt to use less vulnerable cryptographic security mechanisms (e.g., pre-shared symmetric keys or hashing algorithms) in some operational technology because they require fewer computational resources (Stouffer et al., 2015). Networked ICSs often also rely on additional, redundant network security mechanisms that would further mitigate vulnerability, even where long-lived operational technologies were deployed with vulnerable cryptographic security mechanisms (ICS-CERT, 2016). Many cyber-physical systems used in mass transit applications have long lifetimes and could be challenging or costly to update in the field; many of these systems currently use “outdated digital and analog technology” (American Public Transportation Association, 2014, p. 5), and quantum computing vulnerabilities are unlikely to be a priority for mitigation.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in most categories.
References

Works That Informed the Analysis


National Critical Function 19, Conduct Elections

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Medium</td>
<td>Each U.S. state that allows the electronic transmission of ballots should ensure that these transmitted ballots are encrypted using post-quantum cryptography (PQC). Databases for election reporting will also need to adopt PQC in authentication before a cryptographically relevant quantum computer (CRQC) arrives.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Migration is likely to take place through routine, conventional cybersecurity efforts, such as software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
<td>Public trust in the integrity of U.S. elections has decreased in recent years, and the interception and release of even a very small amount of identifiable voter data would further damage public trust in the integrity of the vote.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>The national critical function (NCF) does deal with a very small amount of identifiable data in transit with a long confidentiality lifetime, exacerbated by the U.S. public’s relatively low trust in the integrity of the election system. This is mitigated by the low amount of data, the limited number of organizations that handle those data, and the low cost of mitigating the threat.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td></td>
<td>A small number of overseas U.S. voters from certain states are allowed to transmit their ballots electronically. Although these ballots constitute a tiny fraction of the total, they do have a long confidentiality lifetime and should be protected by PQC as soon as possible. Organizations in the NCF should now begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
</tr>
</tbody>
</table>

CISA definition: “Conduct elections, including managing voter registration and rolls, voting infrastructure, polling places, vote counting, and certifying and publishing election results” (CISA, 2020b, p. 4).

Synopsis of Issues

For the past 100 years, the secret ballot has been a key component of the U.S. election process. The potential for unauthorized disclosure of voters’ ballot choices is the most significant catch-and-exploit vulnerability for this NCF, particularly because this information has a long confidentiality lifetime (at least as long as the voter’s lifetime). A CRQC would pose a low risk to most voters’ ballot secrecy. For voters who vote in person or by mail, the only election results transmitted electronically are from the voting precinct to the local or state jurisdiction, and these data consist of precinct vote totals (which are announced publicly soon after the election) and no personally identifiable information (PII). Most states do, however, allow certain voters to transmit absentee ballots electronically—usually only expatriates and members of the armed forces covered by the federal Uniformed and Overseas Citizens Absentee Voting Act (Pub. L. 99-410, 1986). States vary widely in their allowed methods of vote transmission, including web portals, mobile apps, email, or

---

1 Forty-four U.S. states have constitutional provisions guaranteeing secrecy in voting, and the remaining states have laws that do the same (Fitzgerald, Smith, and Goodman, 2016).

2 We would like to acknowledge Quentin Hodgson of the RAND Corporation for providing subject-matter expertise on this NCF. Recently, there have been several proposals for “end-to-end auditable (or verifiable) voting systems,” in which individual votes are posted publicly in encrypted form, so that each voter can verify the correctness their own vote but no one else’s. If these systems are ever widely adopted, it will be important to ensure that the encryption protocol is quantum safe. However, these systems have been deployed to only an extremely limited degree in U.S. elections (Wofford, 2020).
fax (National Conference of State Legislatures, 2019a). In principle, these transmissions could pose a risk of catch-and-exploit vulnerabilities that could reveal votes, but, in many cases, these transmissions are already unencrypted (MacDonald-Evoy, 2020), so a CRQC would not introduce new vulnerabilities.

A CRQC would create the risk of authentication vulnerabilities in remote network and database access. A threat actor with a CRQC could access or modify databases of registered voters, tallies of votes received from each precinct, and similar data, seriously degrading trust in the integrity of the election process, but this is a just-in-time vulnerability that can be resolved any time before the advent of a CRQC. These authentication vulnerabilities are primarily in software products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services).

Urgency
Our assessment is that urgency of action for this NCF is low overall, with one exception that must be addressed more quickly. The only identified data in transit with a long confidentiality lifetime are the relatively small number of electronic ballots submitted by expatriates and members of the armed forces to the states that allow this form of transmission. The systems that facilitate these transmissions must move to the use of PQC for key exchange once standard PQC algorithms are released. All other systems need not complete the migration until just before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is medium. Each state organization governing elections will need to address vulnerabilities. The only active risk mitigations required are that each U.S. state that allows the electronic transmission of ballots should, as soon as possible after the new algorithms are standardized, ensure that these transmitted ballots are encrypted using PQC.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are exacerbating. Public trust in the integrity of the U.S. electoral systems has decreased in the past decade (Reinhart, 2020; Laughlin and Shelburne, 2021). Although a CRQC poses a low direct risk to the integrity of elections, a breach of voter data of any size—or even a plausible claim of one—could further damage public trust in the electoral system and degrade the functioning of the NCF. The interception and decryption of even a small number of overseas absentee ballots would require a high-resource catch-and-exploit campaign and would probably only reveal a small amount of information. But any public reveal of this information could have large impact on national trust in election security. A threat actor with the resources for a catch-and-exploit campaign might have the motivation to conduct one.

Priority for Assistance
We rated the NCF as a medium priority for assistance because of the presence of a small amount of identifiable data in transit with a long confidentiality lifetime, exacerbated by the U.S. public's relatively low trust in
the integrity of the election system. This is mitigated by the fact that there is only a small amount of sensitive data, the limited number of organizations that handle those data, and the low cost of mitigating the threat.

References

Works That Informed the Analysis
Wofford, Benjamin, “A Texas County Clerk’s Bold Crusade to Transform How We Vote,” Wired, September 15, 2020.

Related Reading
National Critical Function 20, Develop and Maintain Public Works and Services

Category: Manage

Summary

| Urgency   | Low       | Updates can happen gradually, provided that they are complete when a capable quantum computer arrives. |
| Scope     | Low       | Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare. |
| Cost      | Low       | Mitigation is likely to take place through software updates and in-cycle hardware replacement. |
| Other factors | Neutral | We identified no other mitigating or exacerbating factors. |
| Priority for assistance | Low       | Low ratings in all categories lead to a rating of low priority for assistance. |
| Primary concern(s) | Organizations in the NCF should begin early preparations for the post-quantum cryptography (PQC) migration following the U.S. Department of Homeland Security (DHS) roadmap. |

CISA definition: “Design, build, and maintain infrastructure to supply government services, including systems and assets used for transportation and traffic management, water supply, waste management, recreation, and other purposes” (CISA, 2020b, p. 4).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

This NCF will experience authentication vulnerabilities in products and services provided by other NCFs, and it will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. These vulnerabilities arise from the ubiquitous use of public-key cryptography to identify and authenticate users and equipment across the Internet. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer arrives.  

Urgency

Our assessment is that urgency of action for this NCF is low. Internet-dependent business IT products and services will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives.  

---

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business information technology (IT) systems. We assessed that this group included NCFs 20, 21, 26, 27, 31, 36, and 51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.
arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for providing updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are neutral. We identified no additional mitigating or exacerbating factors.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

References
Works That Informed the Analysis
National Critical Function 21, Educate and Train

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Summary</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
<td>Although many issues will be addressed by other national critical functions (NCFs), the fragmentation of educational data systems means that many organizations will need to manage updates themselves.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>We identified no other mitigating or exacerbating factors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>The high number of organizations that might need to address the migration to PQC in their systems leads to a rating of medium priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Organizational network access and remote database access systems must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Provide education and workforce training including PreK–12, community college, university, and graduate education, technical schools, apprenticeships, non-formal education, and on-the-job training” (CISA, 2020b, p. 4).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. The NCF handles sensitive data related to student records and associated personally identifiable information (PII), but these data do not have a long confidentiality lifetime. Federal and state legislation provide regulations on maintaining privacy for student records and associated PII, but it generally does not dictate specific data protection rules.1

This NCF will experience authentication vulnerabilities primarily in shared databases and networked business information technology (IT) systems used in operations. NCF operations often require secure access to shared databases hosted by local, regional, and national organizations (National Center for Education Statistics, undated; von Zastrow and Perez, 2019). These databases could be used to maintain student records, record data and statistics about educational systems, or provide Internet-accessible educational and training material. The NCF requires assured remote access and fidelity of these databases, each of which will require updates to protocols used for secure remote access over the Internet. Many of these databases and other products and services related to networked business IT systems are provided by other NCFs, and this NCF will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. These products and services must migrate to use PQC for remote authentication before a CRQC arrives.2


2 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business IT systems. We assessed that this group included NCFs 20, 21, 26, 27, 31, 36, and
Urgency
Our assessment is that urgency of action for this NCF is low. Database-hosting systems and other Internet-dependent business IT products and services will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is high. Databases and information-sharing systems are managed by hundreds of local school districts and state and federal organizations. Many of the vulnerable networked business IT products and services are provided by other NCFs, and the providers of those products and services will be responsible for their migration to PQC. Where organizations in this NCF rely on third-party database-hosting providers, responsibility for the migration to PQC would similarly fall on those providers in another NCF. Nevertheless, the reported lack of information-sharing and interoperability between educational data systems (von Zastrow and Perez, 2019; Walters, 2020) suggests that a significant portion of affected NCF organizations operate siloed, self-managed information systems, and they will need to take action themselves to adopt PQC for authentication.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are neutral. We identified no additional mitigating or exacerbating factors.

Priority for Assistance
We rated the NCF as a medium priority for assistance because of its high scope, despite low ratings in urgency and cost.

References
Works That Informed the Analysis
Parent Coalition for Student Privacy, "State Student Privacy Laws," webpage, undated.
U.S. Code, Title 15, Commerce and Trade; Chapter 91, Children’s Online Privacy Protection.

51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

———, 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.


National Critical Function 22, Enforce the Law

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Factor</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>High</td>
<td>This national critical function (NCF) handles a significant amount of data in transit with a long confidentiality lifetime.</td>
</tr>
<tr>
<td>Scope</td>
<td>High</td>
<td>This NCF has many, highly dispersed organizations, each of which must individually address updates.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Once a post-quantum cryptography (PQC) standard is available, most organizations will be able to update using readily available updates to protocols and commercial software products.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>This NCF has both exacerbating and mitigating factors, but the balance is mitigating. Exacerbating factors include extant challenges in sharing information and managing information technology updates and likely low threat awareness. Mitigating factors include effective regional and national organizations with missions to assist NCF-affiliated organizations in managing a variety of challenges.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>The NCF has high urgency and broad, dispersed scope of organizations with catch-and-exploit vulnerabilities. That risk is diminished by factors mitigating catch-and-exploit risk and the likely low level of effort required to fix vulnerabilities.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td></td>
<td>A very large number of organizations routinely transmit highly sensitive data with a long confidentiality lifetime. Each will need to individually move to secure those communications with PQC as soon as practical.</td>
</tr>
</tbody>
</table>

CISA definition: “Operate Federal, State, local, tribal, territorial, and private sector assets, networks, and systems that contribute to enforcing laws, conducting criminal investigations, collecting evidence, apprehending suspects, operating the judicial system, and ensuring custody and rehabilitation of offenders” (CISA, 2020b, p. 4).

Synopsis of Issues

NCF operations require the routine, ubiquitous transmission of sensitive information with a long confidentiality lifetime. Organizations providing law enforcement, court services, and institutional and community corrections at the local, state, and federal levels must routinely communicate information on justice-involved people. Sensitive data in transit could include the identities of witnesses and informants, documentation of evidence in criminal investigations, criminal records, and sealed court records. Given the diversity of organization types transmitting this information, security practices for this kind of communication likely vary widely and could create a high risk from catch and exploit. The current use of analog communications or symmetric-key file encryption for file transfers would mitigate most of this vulnerability when used, but vulnerability would be introduced where organizations instead relied on the assumed security in commonplace message and file transfer mechanisms, such as email or secure web portals.

Authentication issues exist for databases, network account access, and cyber-physical systems. NCF operations require secure access to many shared databases hosted by local, regional, and national organizations. The following are just a few examples: repositories of evidence in criminal investigations; data to facilitate investigations, such as license plate databases or biometric records (e.g., fingerprint or facial recognition); court records; criminal records; databases of outstanding warrants; and other data supporting institutional corrections, community supervision, and reentry services. The NCF requires assured remote access and fidelity of these databases, each of which will require updates to protocols used for secure remote access over the Internet. Moreover, it relies on secure remote access to systems that facilitate both routine operations and emergency response, such as those governing dispatches, 911 calls, and even some cyber-physical examples,
such as emergency sirens. Numerous examples already exist of cyberattacks disrupting this NCF by exploiting current vulnerabilities in such systems as those mentioned (Dixon, 2019). Failing to update systems to address risk from quantum computers could lead to many other devastating examples.

**Urgency**

Our assessment is that urgency of action for this NCF is high because of the significant amounts of data in transit with a long confidentiality lifetime. It will also be important to manage updates to the security protocols used to remotely access high-priority databases, but this is a just-in-time risk, and mitigation will be far less urgent than addressing sensitive data in transit. Systems that involve sensitive data in transit now need to move to post-quantum encryption schemes as soon as possible to limit risk. Sensitive data in transit would include documentation of evidence in criminal investigations, criminal records, and sealed court records. All organizations in the NCF should also begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**

Our assessment is that scope is high for this NCF because of the large number of organizations that must make an active, urgent response to mitigate risk. All mechanisms currently used for secure file transfer (e.g., email servers) must be updated with the PQC standard. NCF organizations that are likely to currently be transmitting data with a long confidentiality lifetime include municipalities, police agencies (the United States is often estimated to have 18,000 police agencies; see, e.g., Jackson et al., 2020), court systems, prisons, and probation and parole agencies. It will also include supporting federal agencies and organizations, such as the Federal Bureau of Investigation, the U.S. Drug Enforcement Administration, the Bureau of Prisons, and a plethora of other federal law enforcement–related organizations. In addition to these organizations, those that are managing the many shared databases relied on by all of these organizations must take action to update remote database access protocols.

**Cost**

Our assessment is that cost per organization is low for this NCF. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are mitigating, on balance, although some exacerbating factors apply. Challenges are exacerbated by the fact that many organizations associated with this NCF already find it difficult to keep up with technological change, especially with respect to keeping information technology up to date (Jackson et al., 2020). As a result, most are unlikely to independently make swift updates without external support. Challenges for this NCF are mitigated, however, by the existence of multiple regional and national organizations that already support organizations and research in this space, including federal examples, such as the Office of Justice Programs and its Bureau of Justice Assistance and the National Institute of Justice. These organizations will be useful in efforts to disseminate information, guidance, and other resources to others in the NCF.

Moreover, most organizations in this NCF will not realistically be a high risk because of the factors mitigating risk from catch-and-exploit vulnerabilities. Catch-and-exploit campaigns will require significant investment of resources that will likely be unavailable to most potential threat actors that would be relevant to this NCF. A relatively small number of organizations will need to move quickly to mitigate catch-and-
exploit vulnerabilities where they handle especially sensitive information with a long confidentiality lifetime. These data types would include sealed court records or the identities of witnesses under protection, undercover law enforcement personnel, and law enforcement informants. Data related to U.S. litigation that affects the governments of other countries could similarly be a higher risk from catch and exploit, although the likely shorter confidentiality lifetime of these data could mitigate that risk to a significant degree. Organizations communicating these kinds of data should be the foci for urgent updates to communication systems, while most of the others can be reached over a longer period of time by guidance and trainings from existing supporting organizations over time.

Priority for Assistance
We rated the NCF as a medium priority for assistance. Although catch-and-exploit issues are urgent and cover a very large scope of organizations, realistically, only a tiny fraction of the NCF organizations must be prioritized to address them swiftly. Moreover, a large number of organizations must take actions independently to address issues with catch and exploit and authentication, especially for critical databases on which the NCF relies, but the level of effort required to do so in each case is likely very small and can be accomplished with readily available tools, human capital, and guidance.

References
Works That Informed the Analysis
Priority Criminal Justice Needs Initiative, homepage, undated.
National Critical Function 23, Maintain Access to Medical Records

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>High</th>
<th>This national critical function (NCF) handles a significant amount of protected health information (PHI) with a confidentiality lifetime of many decades.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Medium</td>
<td>A fairly small number of major vendors of electronic health records (EHRs) could push out centralized updates that would cover most PHI transmission between medical facilities, but some specialized medical device and software providers might need to take individual action.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement for most organizations.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Several national and international medical interoperability standard-setting organizations could assist the NCF in managing the transition; threat actors with sufficient resources for a catch-and-exploit campaign are unlikely to target PHI.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>The NCF has high urgency because of the very long confidentiality lifetime of PHI, but the risk is diminished by the limited number of organizations that need to take proactive action and the low cost of doing so.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>PHI has an extremely long confidentiality lifetime that (under current law) extends even beyond a patient’s death. It is likely that a cryptographically relevant quantum computer will be developed while PHI being generated today still remains sensitive.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: "Maintain, use, and share actionable data (including personally-identifiable information and personal health information such as care history) effectively, appropriately, bi-directionally and in a timely fashion, for patient care, billing, and operational and clinical research" (CISA, 2020b, p. 4).

Synopsis of Issues

This NCF exhibits serious catch-and-exploit vulnerabilities. Medical providers routinely share PHI with each other and with EHR vendors. If patients lose trust in the security of their PHI, they will be less willing to share it with medical providers, severely degrading the functioning of the NCF. The negative consequences of such an interception of PHI could include blackmail, the infliction of personal embarrassment, or inappropriate targeted marketing. Regulations governing implementation of the Health Insurance Portability and Accountability Act (Pub. L. 104-191, 1996) require that all covered entities “implement a mechanism to encrypt and decrypt electronic protected health information” (45 C.F.R. § 164.312[a][2][iv]) whenever doing so is a reasonable and appropriate safeguard (Centers for Medicare and Medicaid Services, 2007). Moreover, PHI remains legally protected not only throughout a patient’s entire lifetime but for 50 years after the patient’s death (Office for Civil Rights, 2013), so, under current law, some PHI being generated today could remain sensitive for well over a century. These data are currently routinely transmitted via Internet-mediated products and services (e.g., cloud-based services or EHR software suites) that depend on vulnerable encryption mechanisms for security.

Some authentication vulnerabilities in the NCF relate to providers’ reliance on Internet-based services in their operations, including in remote access to their internal networks. There are also authentication issues for databases containing PHI, which are ubiquitous in medical facilities of all kinds. Already, several major cyberattacks on PHI databases might have exposed the medical records of tens of millions of people (Snell, 2015a; Snell, 2015b). A hostile actor that gains access to these databases could acquire PHI at rest (with the negative consequences described above) or even modify it, although we assess the risk of EHR falsification to be lower than the risk of data access, given the lack of clear motivation to do so. The NCF requires assured...
remote access and fidelity of these databases, each of which will require updates to protocols used for secure remote access over the Internet before an attacker possesses a capable quantum computer.

**Urgency**

Our assessment is that urgency of action for this NCF is high. The exceptionally long confidentiality lifetime of PHI (often well over 100 years) means that it is very likely that a cryptographically relevant quantum computer will be developed while PHI being generated today still remains sensitive. The sooner that medical institutions switch to post-quantum cryptography for data transmitted between them, the less stored data will be vulnerable for decryption. Updating the security protocols for remote access to PHI databases is a just-in-time risk that is much lower urgency. Organizations should begin early preparations for the post-quantum cryptography migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**

Our assessment is that scope for this NCF is medium. A small number (between ten and 100) providers of software products and services will have the primary responsibility for addressing vulnerabilities specific to this NCF (FactSet, 2021). The Health Insurance Portability and Accountability Act contains a security rule that establishes data protection standards for PHI, a portion of which are technical safeguards, including a requirement for encryption (where reasonable and appropriate) (Centers for Medicare and Medicaid Services, 2007). Best practices and guidance for transfer of patient data often discourage the direct transfer of records between care providers and with customers (Adler, 2013; Prodan, 2018). In most cases, medical records are transmitted through centralized enterprise software suites and secure web portals developed by a few major EHR vendors, each of which serves thousands of providers. These products and services will need to make software and configuration changes in their products, which will be pushed out to their customers. Other vulnerabilities associated with use of the Internet to access and deliver data are the responsibility of other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). These large vendors do need to individually develop customized installations of their software for certain specialized clinical software modules and medical devices, however, and, in these specialized cases, smaller medical software or device manufacturers might need to adjust their encryption systems as well, so the major EHR vendors might need to coordinate with these other organizations.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. Most required actions can be achieved through relatively centralized software updates pushed out by a small number of major EHR vendors. These updates would likely involve a relatively low level of effort for vendors, and most medical providers need only to implement these updates. Moreover, medical records are generally transmitted between commercial off-the-shelf computer systems that are replaced at regular cycles. However, there could be a few providers of medical devices or services that need to implement more-extensive mitigations.

---

1 We acknowledge Natalie Ernecoff, Shira Fischer, and Zach Predmore of the RAND Corporation for providing subject-matter expertise on this.
Other Factors
Our assessment is that other factors for this NCF are, on balance, mitigating. Several national and international organizations develop interoperability standards and specifications for the medical industry, such as the Center for Medical Interoperability and Health Level Seven International, which maintains the internationally used Health Level Seven standard for medical data. These organizations will be useful in efforts to disseminate information, guidance, and other resources to others in the NCF.

Depending on their motivations, threat actors could attempt either bulk collection of PHI or targeted collection of a specific person's PHI. A large-scale catch-and-exploit campaign would involve significant practical challenges. A threat actor would likely not know what data were in a bulk capture of data until they actually decrypted the many communication streams. The significant resource requirements needed to do this decryption, combined with the likely low utility of the desired PHI data, would make such a bulk catch-and-exploit campaign unlikely for a realistic threat actor. It might be difficult for even a high-resource threat actor to predict whose medical data will be useful ten or more years in the future, then capture communications about them specifically. We assessed that these considerations significantly mitigate the threat of a catch-and-exploit campaign targeting PHI.

Priority for Assistance
We rated the NCF as a medium priority for assistance because of the exceptionally long confidentiality lifetime of PHI, offset by the relatively small number of major EHR vendors that need to make proactive efforts to convert their cryptography algorithms in order to protect the large majority of EHR transmissions and the low cost of doing so.

References
Works That Informed the Analysis


Code of Federal Regulations, 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.


FactSet, financial data and analytics, 2021.


National Critical Function 24, Manage Hazardous Materials

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Organizational network access and systems that secure industrial control systems must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: Safely identify, monitor, handle, store, transport, use, and dispose of hazardous materials (including chemical, biological, radioactive, nuclear, and explosive substances) under normal operations and in response to emergencies.

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that may be regularly transmitted.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.¹

¹ This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business information technology systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team, 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Urgency
Our assessment is that urgency of action for this NCF is low. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap (DHS, 2021).

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap (DHS, 2021). When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance due to low ratings in all assessed factors.

References
Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.
National Critical Function 25, Manage Wastewater

Category: Manage

Summary

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>The water and wastewater sector is well supported by various groups, and additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Organizational network access and systems that secure ICSs must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: "Collect and treat industrial and residential wastewater to meet applicable public health and environmental standards prior to discharge into a receiving body" (CISA, 2020b, p. 4).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology (IT) products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, process control systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC wherever public-key encryption is used for authentication prior to the arrival of a CRQC.

1 Water and wastewater are typically treated as a single sector, and they share most of the same organizations and vulnerabilities. As a result, the assessments for NCF 25 and NCF 55 are largely identical.

2 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quan-
Urgency
Our assessment is that urgency of action for this NCF is low. Cyber-physical systems and IT network access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low. Although the wastewater sector includes more than 16,500 publicly owned treatment works (DHS and U.S. Environmental Protection Agency [EPA], 2015), it is unlikely that these organizations will need to actively address the vulnerabilities. Most affected products and services are provided by other NCFs, and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. The water and wastewater sector is well supported by many public and private organizations and associations, including the Water and Wastewater Systems Sector Coordinating Council, Water and Wastewater Systems Government Coordinating Council, Water Information Sharing and Analysis Center, and various other affiliated organizations (see DHS and EPA, 2015, Appendix 3). These groups are coordinating to develop cybersecurity resources for the sector, and state and federal regulations are increasingly requiring water system operators to address and prioritize cybersecurity (Germano, 2019). These are collectively seen as a mitigating factor.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

References

Works That Informed the Analysis


**Related Reading**

National Critical Function 26, Operate Government

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Medium</td>
</tr>
<tr>
<td>Scope</td>
<td>High</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Organizations in the NCF should begin early preparations for the post-quantum cryptography (PQC) migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
</tr>
</tbody>
</table>

CISA definition: “Carry out legislative, judicial, and executive government missions, including activities related to developing and enforcing codes, ordinances [sic], rules, regulations, and laws; collecting taxes and revenues; managing records, budgets, and finances; and providing public services” (CISA, 2020b, p. 4).

Synopsis of Issues

To a significant degree, this NCF is a collection of functions from other NCFs. The quantum computing vulnerabilities associated with those functions are discussed in more depth in their assessments, especially NCF 22, Enforce Law; NCF 35, Provide Identity Management and Associated Trust Support Services; NCF 38, Provide Payment, Clearing, and Settlement Services; and NCF 39, Provide Public Safety. This assessment addresses primarily vulnerabilities associated with the communication, data-sharing, and collaboration between government entities needed to develop and enact codes, ordinances, rules, regulations, and laws.

This NCF does handle some information in transit with a moderate confidentiality lifetime, including PII and proprietary business information associated with management of taxes, finances, and provision of public services. These data would generally have a short to medium confidentiality lifetime, and they will exhibit catch-and-exploit vulnerabilities until PQC is used in key exchange to secure data in transit.

This NCF will experience primarily authentication vulnerabilities in shared databases and networked information technology (IT) systems used in a variety of government operations. NCF operations often require secure access to shared databases hosted by local, regional, and national organizations. These databases could be used to store a variety of sensitive PII, financial data, and other public data that must be accessible by appropriate government users. The NCF requires assured remote access and fidelity of these databases, each of which will require updates to protocols used for secure remote access over the Internet. Many of these databases and other products and services related to networked business IT systems are provided by other NCFs, and this NCF will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. Products and services from these NCFs are crucial to secure communication and information-sharing across governments. These vulnerabilities arise from the ubiquitous use of public-
key cryptography to identify and authenticate users across networked systems. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer (CRQC) arrives.\(^1\)

**Urgency**

Our assessment is that urgency of action for this NCF is medium. Operators in the NCF will handle PII and proprietary business information with a moderate confidentiality lifetime. Like other NCFs responsible for protecting PII (except protected health information [PHI]) and proprietary business information, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years), and their protection from catch and exploit justifies an assessment of medium urgency. Internet-dependent IT products and services, including remote access to critical databases, will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is high. The scope includes the federal government and thousands of entities forming municipal, county, and state governments across the United States. Although many of the vulnerable networked IT products and services, including third-party database-hosting services, are provided by other NCFs, if even a small portion of the potential scope self-hosts aspects of their IT infrastructure, the number of affected organizations would be well above the stated threshold for a high scope in the assessment.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are exacerbating. Inhibiting the operation of government can be viewed as a high-value target for a well-resourced nation-state adversary (one of the threat actors we consider likeliest to possess an early CRQC). Even if the federal government acts with appropriate haste to address quantum computing vulnerabilities, the scope in this NCF is high, and states and large municipalities could be seen as targets for disruption. We view this as an exacerbating factor for this NCF.

**Priority for Assistance**

We rated the NCF as a medium priority for assistance because of its high scope and an exacerbating factor, despite low ratings in urgency and cost.

---

\(^1\) This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business IT systems. We assessed that this group included NCFs 20, 21, 26, 27, 31, 36, and 51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.
References

Works That Informed the Analysis

Related Reading
National Critical Function 27, Perform Cyber Incident Management Capabilities

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>The NCF should begin helping its customers prepare for the migration to PQC and assess potential catch-and-exploit vulnerabilities.</td>
</tr>
</tbody>
</table>

CISA definition: “Provide security systems and services that protect critical business assets and functions, including preventive guidance, simulation, testing, and warning capabilities; operate operations response centers and teams; integrate and share information; [and] coordinate and provide response, recovery, and reconstitution services” (CISA, 2020b, p. 5).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit in its own operations. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted. However, prevention of cyber-incidents is one of the main subfunctions of the NCF (U.S. Department of Homeland Security [DHS], 2009), and members of the NCF will need to incorporate guidance and practices related to catch-and-exploit vulnerabilities into the services provided to other NCFs. Members of the NCF will need to stay apprised of the progress in quantum computer development over time to assist customers in assessing related risk. As quantum computing capabilities improve over time, the risk from catch-and-exploit vulnerabilities will grow for customers, and the possibility of a cyberattack enabled by a quantum computer will become more and more likely. Factors related to that attack vector will need to be incorporated into the guidelines, training, and practices of the NCF.

This NCF will experience authentication vulnerabilities in products and services provided by other NCFs, and it will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. These vulnerabilities arise from the ubiquitous use of public-key cryptography to identify and authenticate users and equipment across the Internet. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer arrives.1

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business IT systems. We assessed that this group included NCFs 20, 21, 26, 27, 31, 36, and 52.
Urgency
Our assessment is that urgency of action for this NCF is low, although the NCF should imminently begin to incorporate mitigation of catch-and-exploit vulnerabilities into incident prevention practices and guidance. Internet-dependent business information technology (IT) products and services will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration, both in their own operations and in services provided to customers, by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for making updates available. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. Although the NCF is unlikely to experience urgent vulnerabilities in its own operations, the NCF’s role in preparation and prevention of cybersecurity incidents makes imperative that it quickly incorporate issues associated with quantum computing cybersecurity vulnerabilities and the PQC migration into the services that operators provide to their customers. The NCF will be crucial to efforts to bring broad awareness of quantum computing vulnerabilities and to drive preparation in advance of the release of PQC standards. Fortunately, there is evidence that the NCF has begun to do exactly that: DHS recently published a roadmap for mitigating risk related to quantum computing, and some information-sharing and analysis centers are beginning to address related issues (Witty, 2019). We assessed this to be a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

References
Works That Informed the Analysis
DHS, Information Technology Sector Baseline Risk Assessment, August 2009.

51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.

National Critical Function 28, Prepare for and Manage Emergencies

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>We identified no other mitigating or exacerbating factors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Organizations should follow current cybersecurity best practices and keep products and services that facilitate communication and interoperability up to date as they migrate to use post-quantum cryptography (PQC).

CISA definition: “Organize and manage resources and responsibilities for dealing with all aspects of emergencies (prevent, protect, mitigate, respond, and recover), to be resilient to and reduce the harmful effects of all hazards” (CISA, 2020b, p. 5).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

The NCF will experience authentication vulnerabilities in the wireless and Internet-connected communication services used to coordinate in emergencies. The NCF relies on computer-aided dispatch systems, Next Generation 911 systems, cloud services, and Internet-facilitated communication technologies, among other information technology (IT) and communication technologies (CISA, 2019c). Few other authentication vulnerabilities exist in the architectures for wireless emergency communication, as currently constructed, although future generations might need to address additional vulnerabilities. Emergency wireless communications are a combination of legacy land mobile radio and modernized wireless broadband communication systems, such as the Nationwide Public Safety Broadband Network (CISA, 2019a). Wireless communication devices typically rely on preshared or embedded symmetric keys for security (where encryption is used at all), and these communications are therefore already inherently quantum resistant. Future emergency communication networks are expected to prioritize interoperability and rely on open standards for implementation (Parkinson, 2020). Some security mechanisms, especially those used in fifth-generation (5G) networks, use public key–based authentication to identify user equipment, and these will present an authentication vulnerability until they adopt PQC (Mitchell, 2020). The Nationwide Public Safety Broadband Network, specifically, allows the use of public-key infrastructure in client security management (Local Control Working Group, 2015), and this would present an authentication vulnerability until updated with post-quantum

---

1 There is significant overlap between the communication systems used for provision of public safety and for emergency response, and this assessment therefore shares many similarities with that for NCF 39, Provide Public Safety.

2 Many of the issues associated with wireless broadband networks are discussed in more detail in the assessment for NCF 8, Provide Wireless Access Network Services.
protocols. Like many other organizations, emergency response organizations will face authentication vulnerabilities in networked IT systems, and they will depend on other NCFs (specifically, NCF 3 and NCF 52) to provide relevant updates to those products and services. These vulnerabilities arise from the ubiquitous use of public-key cryptography to identify and authenticate users and equipment across the Internet. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer arrives.

**Urgency**
Our assessment is that urgency of action for this NCF is low. Internet-dependent business IT products and services will need to be updated over time through software updates, security patches, and in-cycle hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for providing updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**
Our assessment is that other factors for this NCF are neutral. We identified no additional mitigating or exacerbating factors.

**Priority for Assistance**
We rated the NCF as a low priority for assistance because of low ratings in all assessed factors.

**References**
Works That Informed the Analysis
———, *Emergency Services Sector Landscape*, August 2019c.
DHS, "Emergency Services Sector Profile," November 2017b.

**Related Reading**
CISA, "Emergency Services Sector Cybersecurity Initiative," webpage, undated.
National Critical Function 29, Preserve Constitutional Rights

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Situations requiring active, swift mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Migration is likely to take place through routine, conventional cybersecurity efforts, such as software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>We did not identify any other factors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Some constitutional processes, such as conducting elections, collecting taxes, and law enforcement, display vulnerabilities to a cryptographically relevant quantum computer (CRQC), but these vulnerabilities are discussed in more detail in the assessments of other national critical functions (NCFs).

CISA definition: “Secure the principles of freedom and independence and maintain the structures of American government through the protection of rights and processes prescribed in the U.S. Constitution” (CISA, 2020b, p. 5).

Synopsis of Issues

In the modern era, many constitutional rights and processes are indirectly supported by broadly available public-key encryption, but we did not identify any rights or processes with functions directly vulnerable to an attacker possessing a quantum computer and not covered by any other NCF.

Table B.1 lists several constitutional rights and procedures with cryptography-related issues discussed in more detail in our discussions of assessments of other NCFs.

**TABLE B.1**

Constitutional Rights and Procedures

<table>
<thead>
<tr>
<th>Topic</th>
<th>Location in the U.S. Constitution</th>
<th>Relevant NCF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducting elections</td>
<td>Article I, §§ 1–4, Article II, § 1, Amendments 12, 14, 15, 17, 19, 20, 22, 23, 24, and 26</td>
<td>NCF 19, Conduct Elections</td>
</tr>
<tr>
<td>Collecting taxes and issuing debt</td>
<td>Article I, §§ 7–8, Amendment 16</td>
<td>NCF 38, Provide Payment, Clearing, and Settlement Services</td>
</tr>
<tr>
<td>Regulate commerce</td>
<td>Article I, § 8, Amendment 16</td>
<td>—</td>
</tr>
<tr>
<td>Promoting science</td>
<td>Article I, § 8</td>
<td>NCF 54, Research and Development</td>
</tr>
<tr>
<td>Waging war</td>
<td>Article I, § 8, Article II, § 2</td>
<td>NCF 53, Provide Materiel and Operational Support to Defense</td>
</tr>
<tr>
<td>Trial by jury</td>
<td>Article III, § 2, Amendments 5–7 and 11</td>
<td>NCF 22, Enforce Law</td>
</tr>
</tbody>
</table>
Outside of the topics listed in the table, the routine, day-to-day unclassified functioning of the legislative, executive, and judicial branches, the structure of which is laid out in the Constitution, do not have significant catch-and-exploit vulnerabilities.¹

Although authentication vulnerabilities pose risks to the operations of all three branches of government, these are just-in-time risks that can be addressed at any time before the advent of a CRQC. These vulnerabilities are likely to be addressed in products and services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services).

**Urgency**

Our assessment is that urgency of action for this NCF is low. Systems used to enable basic government functions outside of the ones listed in the table will need to migrate to post-quantum cryptography (PQC) over time, but these systems need complete the migration only prior to the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**

Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for providing updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

We did not identify any other significant exacerbating or mitigating factors.

**Priority for Assistance**

We rated the NCF as a low priority for assistance because of its low ratings in all categories.

**References**

Works That Informed the Analysis


¹ All transmission of classified information is covered under our discussion of NCF 53, Provide Materiel and Operational Support to Defense.
National Critical Function 30, Protect Sensitive Information

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>High</td>
</tr>
<tr>
<td>Scope</td>
<td>High</td>
</tr>
<tr>
<td>Cost</td>
<td>High</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>High</td>
</tr>
</tbody>
</table>

Sensitive data with a long confidentiality lifetime will not be protected if action is not taken soon, and the broader migration to post-quantum cryptography (PQC) will likely span decades.

Every national critical function (NCF) is affected in some way, and thousands of organizations will be affected in the NCFs most critical to this function.

Significant research, development, testing, and deployment efforts will be required among the most-affected NCFs.

Lack of broader awareness of the issues associated with quantum computing vulnerabilities could exacerbate the challenge, but ongoing government efforts offset this.

High ratings in all categories lead to a rating of high priority for assistance. This priority refers to the need for ongoing coordination, standardization, and information-sharing that benefit all of the NCFs.

- Organizations should begin preparations for the release of the PQC standard, especially by inventorying each instance of public-key cryptography usage in their operations.
- Once the PQC standard is released, PQC needs to be implemented for key exchange anywhere sensitive data with a long confidentiality lifetime are transmitted.
- The relevant NCFs need to provide products and services that enable PQC as soon as practical to allow other NCFs to begin the migration to PQC.

CISA definition: “Safeguard and ensure the integrity of information whose mishandling, spillage, corruption, or loss would harm its owner, compromise national security, or impair competitive or economic advantage” (CISA, 2020b, p. 5).

Synopsis of Issues

Any of the vulnerabilities addressed in each of the other NCF assessments can lead to potential failures to perform this critical function. Wherever in critical infrastructure that an attacker with a quantum computer could exploit those vulnerabilities, the attacker’s target would have failed to protect sensitive information. The specific vulnerabilities exhibited in each NCF are addressed in their assessments, and this assessment addresses the major issues only in generalities.

With respect to quantum computing vulnerabilities, this NCF is most dependent on the migration to PQC occurring in NCF 3, Provide Internet Based Content, Information, and Communication Services; NCF 35, Provide Identity Management and Associated Trust Support Services; and NCF 52, Provide Information Technology Products and Services. These NCFs provide some of the most-important resources for safeguarding remote access to sensitive information, especially through the use of public-key cryptography algorithms in digital signatures, key exchange, and file encryption. Every NCF is at least somewhat dependent on these NCFs for the products and services that facilitate encryption of sensitive communications and data. The robust migration to PQC in those products and services will be required to mitigate nearly every conceivable variety of catch-and-exploit and authentication vulnerability in the NCFs.

Urgency

Our assessment is that urgency of action for this NCF is high. Every information technology product that facilitates the encrypted transmission of sensitive data with a long confidentiality lifetime across networked
Preparing for Post-Quantum Critical Infrastructure

systems will need to migrate to use the PQC standard for key exchange as soon as practical. The responsibility for the provision of products and services that are enabled to use PQC in key exchange will fall primarily on NCF 3 and NCF 52. In addition to those two NCFs, NCF 35 will have a major role in the migration to the PQC standard in digital signatures and digital certificates across U.S. infrastructure, which must happen before a cryptographically relevant quantum computer arrives. Organizations in every other NCF should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

Scope
Our assessment is that scope for this NCF is high. The reliance on secure networked communications and information technology infrastructure is ubiquitous. Every NCF will be affected in some way by the vulnerability that quantum computing capabilities will create in the ability of critical infrastructure to protect sensitive information. The NCFs that are most relevant to this assessment of scope are NCFs 3, 35, and 52, and thousands of organizations across those NCFs will likely need to take significant action to migrate to PQC.

Cost
Our assessment is that scope for this NCF is high. This rating includes assessed cost per organization only in NCFs 3, 35, and 52. For these three NCFs, costs are likely to include significant research and standardization efforts, extensive software development and testing, and widespread hardware development and replacement. Beyond these three NCFs, so many organizations will be affected across U.S. critical infrastructure in such widely differing ways that no useful assessment of cost per organization across all NCFs would be possible. For some NCFs, the actions that allow them to continue to protect sensitive information will be almost completely beneath their visibility as the migration to PQC occurs through routine software updates and in-cycle hardware refreshes, while others could see more-substantial costs, as described in the assessments for those NCFs.

Other Factors
Our assessment is that other factors for this NCF are neutral. Cybersecurity is a complex, nationwide problem, and the United States is currently grappling with how to address conventional cybersecurity issues. The inadequacy of the fragmented, incremental way it has been approached has spurred some to call for a cyber moonshot that would be more strategic and transformational in nature (National Security Telecommunications Advisory Committee, 2018). In this challenging environment, the vulnerabilities from quantum computing can be viewed as a lower-priority, further-into-the-future threat than the devastating conventional threats being addressed now (Vermeer and Peet, 2020). This perspective, although potentially valid for many NCFs, will likely distract from the real, urgent catch-and-exploit vulnerabilities many NCFs exhibit and the need to begin a robust migration to PQC across the United States. The migration to PQC will likely take decades. If sensitive data with a long confidentiality lifetime are not protected now, and, if preparation for the migration to the PQC standard does not begin quickly, the challenge of protecting sensitive information will be multiplied by a new attack vector layered on top of existing conventional vulnerabilities. The lack of priority and awareness of the real vulnerability from quantum computing would be assessed as an exacerbating factor, but this is offset by ongoing U.S. government efforts that support more optimism. The National Institute for Standards and Technology PQC standardization project (Computer Security Resource Center, 2021a) and DHS efforts to prepare critical infrastructure for the migration to PQC (DHS, 2021) are two such examples. Overall, we assessed this information as neutral.
Priority for Assistance
We rated the NCF as a high priority for assistance. This rating applies primarily to relevant organizations in NCFs 3, 35, and 52, and it is due to high ratings in all categories. Although many organizations in these NCFs are already taking adequate actions and might not need technical assistance, government coordinating efforts, standardization, and information-sharing across the NCFs will continue to be beneficial.

References
Works That Informed the Analysis
National Critical Function 31, Provide and Maintain Infrastructure
Category: Manage

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>We identified no other mitigating or exacerbating factors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Organizations in the NCF should begin early preparations for the post-quantum cryptography (PQC) migration following the U.S. Department of Homeland Security (DHS) roadmap.


Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

This NCF will experience authentication vulnerabilities in products and services provided by other NCFs, and it will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. These vulnerabilities arise from the ubiquitous use of public-key cryptography to identify and authenticate users and equipment across the Internet. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer arrives.¹

Urgency

Our assessment is that urgency of action for this NCF is low. Internet-dependent business IT products and services will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

¹ This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business information technology (IT) systems. We assessed that this group included NCFs 20, 21, 26, 27, 31, 36, and 51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.
Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for making updates available. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are neutral. We identified no additional mitigating or exacerbating factors for this NCF.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

References
Works That Informed the Analysis
National Critical Function 32, Provide Capital Markets and Investment Activities

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Organizations involved in this national critical function (NCF) transmit sensitive commercial and personal data that have a moderate confidentiality lifetime.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other NCFs. Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Migration is likely to take place through routine, conventional cybersecurity efforts, such as software updates and in-cycle hardware replacement, for the most part, although some specialized systems could require more-complex upgrades.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
<td>The financial sector is a likely target, and even rare attacks could cause systemic disruption. These factors are offset by existing regulatory structure and proactive efforts that could facilitate the migration to post-quantum cryptography (PQC).</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
<td>Medium urgency and exacerbating factors contribute to a medium priority for assistance, despite low scope and cost.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>After the arrival of a cryptographically relevant quantum computer (CRQC), a threat actor could gain database access or generate unauthorized trades of securities, potentially greatly harming public trust in the reliability of the stock, bond, and derivative markets.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Issue and trade securities, including debt securities (such as bonds), equities (such as stocks), and derivatives (such as options and futures); provide advisory services and related services, such as prime brokerage; maintain [and] operate organized markets and over-the-counter mechanisms for these instruments” (CISA, 2020b, p. 5).

Synopsis of Issues

The NCF will experience moderate catch-and-exploit vulnerabilities. The NCF handles some sensitive data, such as material nonpublic financial information about companies, valuable IP held on behalf of clients, and records of individuals’ or corporations’ trades of stocks, bonds, and derivatives. These data would generally have a short to medium confidentiality lifetime, and they will exhibit catch-and-exploit vulnerabilities until PQC is used to secure data in transit.

Like other NCFs pertaining to the financial services sector, this NCF will exhibit severe authentication vulnerabilities.1 The financial service sector is a highly interconnected ecosystem of various financial institutions, markets, exchanges, and third-party service providers. The use of public-key cryptography to facilitate remote access to financial services (including authentication of financial transactions) is commonplace in the financial sector (Deodoro et al., 2021; Federal Financial Institutions Examination Council, 2016). A threat actor in possession of a quantum computer could forge digital signatures or digital certificates and initiate counterfeit transactions of various financial assets to either steal those assets or manipulate markets. Such an actor could also exploit vulnerabilities to achieve remote access to the internal networks of financial institutions. Even if these vulnerabilities were only rarely exploited, a few well-publicized incidents could greatly shake investor confidence in the reliability of the securities market, potentially degrading the functioning

---

1 The authentication vulnerabilities described here are largely shared by each of the NCFs connected to the financial sector: NCFs 32, 33, 34, 38, and 40.
of the entire market (Healey et al., 2018; Eisenbach, Kovner, and Lee, 2021). These vulnerabilities need to be addressed only before a CRQC is available.

**Urgency**
Our assessment is that urgency of action for this NCF is medium. Financial securities trading organizations do frequently transmit sensitive data containing proprietary business information, company financial information, and records of securities trades. Some of these data will have a moderate confidentiality lifetime (i.e., one to ten years), and organizations will need to adopt PQC in key exchange to protect these data in communications within a few years of the release of the PQC standard. Public-key algorithms used to ensure authentication and nonrepudiation of financial transactions (e.g., digital signatures) will also need to migrate to use PQC algorithms. Internet-dependent business information technology products and services will also need to be updated over time through software updates, security patches, and hardware replacements, but systems need not complete those updates until just prior to the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**
Our assessment is that scope for this NCF is low. Although the Financial Industry Regulatory Authority (FINRA) reported that there were 3,835 registered brokerage firms and exchange markets in the United States in 2021 (FINRA, 2021), these organizations will likely not need to take significant action to address vulnerabilities. Most affected products and services are provided by other NCFs, and those NCFs will be responsible for providing updates via software updates and hardware products that enable PQC by default. As a result, appropriate actions (e.g., configuring commercial products to use PQC in key exchange) from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**
Our assessment is that cost per organization for this NCF is low for the most part. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. For most securities trading hardware and software, migration to PQC is likely to take place as part of routine, conventional cybersecurity efforts, such as software updates, security patches, and in-cycle hardware replacement. However, certain specialized systems might require more-complex replacements or even system redesigns. For example, high-frequency trading is often implemented over highly specialized hardware (Lockwood et al., 2012). Depending on how encryption is integrated with these systems, they might be more expensive to replace.

---

2 Like with many other assessments, we assumed that information technology products and services that enable the migration to PQC would be available quickly after the completion of the National Institute of Standards and Technology PQC standardization project and that organizations can therefore wait until the planned end of life of hardware to replace it with a PQC-compatible version. In case this assumption does not hold true, Petrenko, Mashatan, and Shirazi, 2019, provides a detailed estimate of the high cost for a large financial institution to perform an off-cycle hardware migration to accommodate PQC.

3 Like with many other assessments, we assumed that information technology products and services that enable the migration to PQC would be available quickly after the completion of the National Institute of Standards and Technology PQC standardization project and that organizations can therefore wait until the planned end of life of hardware to replace it with a PQC-compatible version. In case this assumption does not hold true, Petrenko, Mashatan, and Shirazi, 2019, provides a detailed estimate of the high cost for a large financial institution to perform an off-cycle hardware migration to accommodate PQC.
Other Factors
Our assessment is that other factors for this NCF are exacerbating, on balance, with mitigating and exacerbating factors present. The U.S. securities market is externally regulated by a dedicated federal agency, the U.S. Securities and Exchange Commission, and self-regulated by the private FINRA. These organizations have significant regulatory authority over the finance sector and could help promote a deliberate and uniform industrywide transition to PQC. The financial sector has also been notably aware of the issues created by quantum computing and proactive in preparing for the migration to PQC (Castellanos, 2020; Eisenbach, Kovner, and Lee, 2021; Toshiba Corporation, 2020). We assessed these to be mitigating factors.

The potential ability to directly steal financial assets is likely to make financial institutions high-value targets for most potential threat actors. Banking is often the industry most affected by cybercrime (Bissell, LaSalle, and Dal Cin, 2019). Although impersonation attacks that allow counterfeit transactions are an authentication vulnerability that needs to be addressed only just before a CRQC is available, it is likely that such attacks would be among the first attempted by an attacker with the capability to do so. There is therefore likely to be little room for delay in the migration to PQC in the financial sector. Furthermore, the interconnected nature of the financial system and the shared technological vulnerability from quantum computing make it likely that even a rare successful attack could lead to systemic shocks that could significantly degrade the function (Eisenbach, Kovner, and Lee, 2021). We assessed these to be exacerbating factors.

Priority for Assistance
We rated the NCF as a medium priority for assistance. Expected cost and scope are low. Urgency is rated as medium because of the NCF’s potential catch-and-exploit vulnerabilities. Although existing regulatory structure and proactive preparation by the NCF mitigate vulnerabilities, the likelihood that this NCF will be a target of attacks that could cause significant systemic disruption is a significant exacerbating factor. Overall, we rated this NCF as a medium priority for assistance.

References
Works That Informed the Analysis


Related Reading
National Critical Function 33, Provide Consumer and Commercial Banking Services

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Situations requiring active, swift mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Migration is likely to take place through routine, conventional cybersecurity efforts, such as software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>One global trade organization has helped coordinate upgrades to one important component of this national critical function (NCF) (automated teller machines [ATMs]). Although low account asset values (relative to other financial NCFs) could make this NCF a lower-priority target, theft of financial assets are likely to be among the first attempted attacks by an attacker with a cryptographically relevant quantum computer (CRQC).</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

After the advent of a CRQC, a threat actor could erase or modify the records of bank account deposit totals or generate unauthorized withdrawals if the migration to post-quantum cryptography (PQC) is not complete. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: "Accept and maintain deposit accounts (e.g., checking and savings accounts) and close substitutes (e.g., short-term retail notes) from non-financial intermediaries" (CISA, 2020b, p. 5).

Synopsis of Issues

This discussion covers cryptography issues concerning the storage of funds only within deposit accounts. Issues involving the electronic transfer of funds between deposit accounts are covered in our discussion of NCF 38, Provide Payment, Clearing, and Settlement Services.

This NCF will not experience significant catch-and-exploit vulnerabilities. Although the NCF handles sensitive data, such as the total level of funding in an individual’s bank accounts and the timing of deposits and withdrawals, these data are likely to have a short confidentiality lifetime. We identified no other potential catch-and-exploit vulnerabilities.

Like other NCFs pertaining to the financial service sector, this NCF will exhibit severe authentication vulnerabilities.¹ The finance sector is a highly interconnected ecosystem of various financial institutions, markets, exchanges, and third-party service providers. The use of public-key cryptography to facilitate remote access to financial services (including authentication of financial transactions) is commonplace in the financial sector (Deodoro et al., 2021; Federal Financial Institutions Examination Council, 2016). A threat actor in possession of a quantum computer could forge digital signatures or digital certificates and initiate counterfeit transactions of various financial assets to either steal those assets or manipulate markets. This NCF must address this vulnerability specifically in ATM networks, in which public-key cryptography is often used to facilitate key loading onto machines (Close, 2019). An attacker could exploit this vulnerability to load its

¹ The authentication vulnerabilities described here are largely shared by each of the NCFs connected to the financial sector: NCFs 32, 33, 34, 38, and 40.
own keys and steal funds or monitor user traffic on the network. An actor could also exploit vulnerabilities to achieve remote access to the internal networks of financial institutions. Even if these vulnerabilities were only rarely exploited, a few well-publicized incidents could greatly shake confidence in the reliability of commonplace consumer and commercial banking services, especially online banking, potentially degrading the functioning of the entire NCF (Eisenbach, Kovner, and Lee, 2021; Healey et al., 2018). These vulnerabilities need to be addressed only before a CRQC is available.

**Urgency**

Our assessment is that urgency of action for this NCF is low. There is little personally identifiable information (PII) or sensitive data with a long confidentiality lifetime covered under this NCF, so these systems need complete the migration only prior to the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is low. Situations requiring active, swift risk mitigation are likely to be rare in this NCF. Appropriate actions from organizations in this NCF will be minor in scope and are likely to happen over time with limited engagement.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are neutral, on balance, with mitigating and exacerbating factors present. One global trade association, the ATM Industry Association, that could help coordinate and provide technical assistance to ATM operators in the transition to PQC. The association has facilitated the global coordination of ATM operating system upgrades, so there is some precedence for this kind of coordination and assistance (ATM Marketplace, 2015). The financial sector has also been notably aware of the issues created by quantum computing and proactive in preparing for the migration to PQC (Castellanos, 2020; Eisenbach, Kovner, and Lee, 2021; Toshiba Corporation, 2020). We assessed these to be mitigating factors.

The potential ability to directly steal financial assets is likely to make financial institutions high-value targets for most potential threat actors. Banking is often the industry most affected by cybercrime (Bissell, LaSalle, and Dal Cin, 2019). Although impersonation attacks that allow counterfeit transactions are an authentication vulnerability that needs to be addressed only just before a CRQC is available, it is likely that

---

2 Like in many other assessments, we assumed that information technology products and services that enable the migration to PQC will be available quickly after the completion of the National Institute of Standards and Technology’s PQC standardization project and that organizations can therefore wait until the planned end of life of hardware to replace it with a PQC-compatible version. In case this assumption does not hold true, Petrenko, Mashatan, and Shirazi, 2019, attempts to provide a detailed estimate of the high cost for a large financial institution to perform an off-cycle hardware migration to accommodate PQC.

3 The authentication vulnerabilities described here are largely shared by each of the NCFs connected to the financial sector: NCFs 32, 33, 34, 38, and 40.
such attacks would be among the first attempted by an attacker with the capability to do so (although the relatively low asset value in the accounts covered by this NCF could make it a less appealing target). Therefore, there is likely to be little room for delay in the migration to PQC in the financial sector. Furthermore, the interconnected nature of the financial system and the shared technological vulnerability from quantum computing make likely that even a rare successful attack could lead to systemic shocks that could significantly degrade the function (Eisenbach, Kovner, and Lee, 2021). We assessed these to be exacerbating factors.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all categories.

References
Works That Informed the Analysis
ATM Marketplace, “Skip to Windows 10 for Next ATM OS Migration, ATMIA Recommends,” June 1, 2015.

Related Reading
National Critical Function 34, Provide Funding and Liquidity Services

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Summary</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Medium</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
</tr>
</tbody>
</table>

This national critical function (NCF) regularly handles financial personally identifiable information (PII) and proprietary business information with a moderate confidentiality lifetime. The most-sensitive information, credit ratings, is maintained by only three accredited organizations nationwide. Migration is likely to take place through conventional cybersecurity efforts, such as software updates and hardware replacement, although perhaps in an accelerated time frame. The financial sector is a likely target, and even rare attacks could cause systemic disruption. These factors are offset by existing regulatory structure and proactive efforts that could facilitate the migration to post-quantum cryptography (PQC).

Primary concern(s)

After the arrival of a cryptographically relevant quantum computer (CRQC), a threat actor could initiate fraudulent transactions or access or modify internal bank databases containing records on corporate or individual customers. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Provide funding to non-financial counterparties, such as corporate or retail customers, including individual consumers” (CISA, 2020b, p. 5).

Synopsis of Issues

This NCF does handle some information in transit with a moderate confidentiality lifetime. Before issuing a loan, financial institutions will typically do due diligence in the form of a credit check or similar investigation of the applicant’s credit risk. In the case of an individual, this information will include sensitive PII; in the case of a business, it could include proprietary financial data (Deodoro et al., 2021). Although the sensitivity of this information decreases over time, it can remain sensitive for many years. An exposure of these data could decrease trust in the credit process, degrading the performance of the NCF. A similar breach to the Equifax credit reporting agency’s records caused the agency to pay at least $575 million in damages (Federal Trade Commission, 2019). The transmission of this information will present a catch-and-exploit vulnerability until communications adopt PQC for key exchange.

Like other NCFs pertaining to the financial services sector, this NCF will exhibit severe authentication vulnerabilities. The finance sector is a highly interconnected ecosystem of various financial institutions, markets, exchanges, and third-party service providers. The use of public-key cryptography to facilitate remote access to financial services (including authentication of financial transactions) is commonplace in the financial sector (Deodoro et al., 2021; Federal Financial Institutions Examination Council, 2016). A threat actor in possession of a quantum computer could forge digital signatures or digital certificates and initiate counterfeit transactions of various financial assets to either steal those assets or manipulate markets. Such an actor could also exploit vulnerabilities to achieve remote access to the internal networks of financial institu-

---

1 The authentication vulnerabilities described here are largely shared by each of the NCFs connected to the financial sector: NCFs 32, 33, 34, 38, and 40.
tions. Even if these vulnerabilities were only rarely exploited, a few well-publicized incidents could greatly shake investor confidence in the reliability of funding and liquidity services, potentially degrading the functioning of the entire market (Eisenbach, Kovner, and Lee, 2021; Healey et al., 2018). These vulnerabilities need to be addressed only before a CRQC is available.

**Urgency**

Our assessment is that urgency of action for this NCF is medium. It regularly handles financial PII and proprietary business information (potentially including sensitive trade secrets). Like in other NCFs responsible for protecting PII (except protected health information [PHI]) and commercial trade secrets, these data are considered to have a moderate confidentiality lifetime (i.e., one to ten years), and their protection from catch and exploit justifies an assessment of medium urgency. Public-key algorithms used to ensure authentication and nonrepudiation of financial transactions (e.g., digital signatures) will also need to migrate to use PQC algorithms. Internet-dependent business information technology (IT) products and services will also need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete those updates only prior to the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is low. U.S. credit checks are centralized into three federally recognized credit rating agencies: Equifax, Experian, and TransUnion (USA.gov, 2021). These three agencies will need to ensure that their transmission of credit scores and other PII transitions to PQC as soon as feasible. Most other financial institutions will not need to take significant, urgent action to address vulnerabilities.\(^2\) Most affected products and services are provided by other NCFs, and those NCFs will be responsible for providing updates via software updates and hardware products that enable PQC by default. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are exacerbating, on balance, with mitigating and exacerbating factors present. The U.S. securities market is externally regulated by dedicated federal agencies, the U.S. Securities and Exchange Commission and the Federal Deposit Insurance Corporation, and self-regulated by the private Financial Industry Regulatory Authority. These organizations have significant regulatory authority over the finance sector and could help promote a deliberate and uniform industrywide transition to PQC. The financial sector has also been notably aware of the issues created by quantum computing and proactive strategies to mitigate these risks.

---

\(^2\) Like with many other assessments, we assumed that IT products and services that enable the migration to PQC will be available quickly after the completion of the National Institute of Standards and Technology's PQC standardization project and that organizations can therefore wait until the planned end of life of hardware to replace it with a PQC-compatible version. In case this assumption does not hold true, Petrenko, Mashatan, and Shirazi, 2019, provides a detailed estimate of the high cost for a large financial institution to perform an off-cycle hardware migration to accommodate PQC.
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

in preparing for the migration to PQC (Castellanos, 2020; Eisenbach, Kovner, and Lee, 2021; Toshiba Corporation, 2020). We assessed these to be mitigating factors.

The potential ability to directly steal financial assets is likely to make financial institutions high-value targets for most potential threat actors. Banking is often the industry most affected by cybercrime (Bissell, LaSalle, and Dal Cin, 2019). Although impersonation attacks that allow counterfeit transactions are an authentication vulnerability that needs to be addressed only just before a CRQC is available, it is likely that such attacks would be among the first attempted by an attacker with the capability to do so. There is therefore likely to be little room for delay in the migration to PQC in the financial sector. Furthermore, the interconnected nature of the financial system and the shared technological vulnerability from quantum computing make it likely that even a rare successful attack could lead to systemic shocks that could significantly degrade the function (Eisenbach, Kovner, and Lee, 2021). We assessed these to be exacerbating factors.

Priority for Assistance

We rated the NCF as a medium priority for assistance. Expected cost and scope are low. We rated urgency as medium because of potential catch-and-exploit vulnerabilities. Although existing regulatory structure and proactive preparation by the NCF mitigate vulnerabilities, the likelihood that this NCF will be a target of attacks that could cause significant systemic disruption is a significant exacerbating factor. Overall, we rated this NCF as a medium priority for assistance.

References

Works That Informed the Analysis


USA.gov, “Credit Reports and Scores,” webpage, October 1, 2021.

**Related Reading**

National Critical Function 35, Provide Identity Management and Associated Trust Support Services

Category: Manage

Summary

| Urgency   | Medium | Some identity verifiers could transmit data with a moderate confidentiality lifetime, but most organizations need to make updates only before a cryptographically relevant quantum computer (CRQC) is available. |
| Scope     | High   | Scope includes hundreds of organizations, including certificate authorities, organizations managing private public-key infrastructure (PKI), and the entire extended ecosystem of identity management services. |
| Cost      | Low    | Most organizations will need only to have certificates reissued over a period of many years. |
| Other factors | Mitigating | This national critical function (NCF) shows significant evidence of collaboration and preparation to address this issue in a highly standard and interoperable manner. |
| Priority for assistance | Medium | Although scope is high, costs are low, organizations have time to implement changes, and the industry is well prepared to make changes when a post-quantum cryptography (PQC) standard is available. |
| Primary concern(s) | Organizations managing their own PKI (especially credential providers, such as those for personal identity verification or common access card) might find the migration most challenging, given the many certificates they will individually be responsible to reissue after a new standard is implemented. |

CISA definition: “Produce and provide technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions” (CISA, 2020b, p. 5).

Synopsis of Issues

The NCF will experience catch-and-exploit vulnerabilities, but identity management is a constantly evolving ecosystem that makes it challenging to assess the severity of a potential catch-and-exploit vulnerability. Those in the NCF seem to recognize that the current paradigm using aggregated personal information and knowledge-based verification for identity verification is inadequate, but it is not yet clear what might take its place (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 lifetimes (e.g., social security number) might be phased out of use in identity verification (Better Identity Coalition, 2018). As a result, PII might not have a long confidentiality lifetime (i.e., greater than ten years), but it could still be vulnerable to catch and exploit on a shorter timescale.

In online authentication, “it is an anomaly when a breach occurs and identity is not the attack vector” (Better Identity Coalition, 2018, p. 26), and this NCF provides the products and services for managing identity. As a result, it is likely the most critical NCF for addressing broader quantum computing vulnerabilities in authentication. Broadly speaking, authentication across networked information systems, such as the Internet, is often managed by associating a public cryptographic key with an entity with a verified identity (Kessler, 2021).1 A user can prove their association with that verified identity by being able to use the corre-

---

1 More generally, authentication is managed by the sharing of secret information known only by the intended parties, such as a username and password combination. Public-key cryptography provides a means of securely sharing secret information
Preparing for Post-Quantum Critical Infrastructure

Corresponding private key (known only to them) to decrypt information encrypted with the associated public key (also known as a digital signature; see IT Laboratory, 2019). The association of identity with a public key often occurs via the issuance of a digital certificate that lists the public key alongside verified identifying information. Certificates are issued by trusted certificate authorities (CAs) within PKI identity management systems. CAs and registration authorities (local agents employed by CAs to verify user identities) form the root, or anchor, for chains of trust in identity management for much of the Internet ecosystem, all facilitated by digital certificates (U.S. Department of Homeland Security [DHS], 2009). These systems can function effectively because (1) users can trust the authorities that verify identities and bind them to public keys and (2) it is practically infeasible for other parties to computationally derive a private key from a strong public key. A CRQC will break the latter criterion by making it feasible to break current public-key cryptography algorithms and derive the private keys. This will create a vulnerability in one of the foundations of authentication and identity management in networked information technology systems. Every digital certificate using the current standard will need to be reissued using a post-quantum standard for digital certificates. Next-generation authentication efforts (e.g., Fast Identity Online or decentralized identifiers) also depend on public-key cryptography and digital signatures, and they, too, will need to migrate to the use of the PQC standard for digital signatures (Commission on Enhancing National Cybersecurity, 2016; Sporny et al., 2021).

Urgency
Our assessment is that urgency of action for this NCF is medium. The NCF will need to incorporate the new PQC standards for digital signatures and digital certificates in existing standards (e.g., a replacement for the widely used digital certificate standard, X.509; see International Telecommunication Union, 2019) and the products and services that use them for authentication services. The update of authentication products and services and reissuance of digital certificates need to happen only before a CRQC exists. It is unclear what personally identifiable information (PII) data will be used, and how, to verify one’s identity a decade or more from now. There appears to be widespread recognition that the current paradigm using aggregated personal information; presumed confidential identifiers, such as social security numbers; and knowledge-based verification is inadequate, but it is not yet clear what could take its place (Better Identity Coalition, 2018). As a result, we assessed that data captured now would not have a long confidentiality lifetime but could have a moderate confidentiality lifetime (one to ten years). This leads to an assessment of medium urgency. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is high. Every CA will need to adopt a new PQC standard for issued certificates. Mozilla’s Common CA Database (Mozilla, undated) alone includes well over a hundred root or intermediate CAs that would be affected, and many others not listed in that database would also need to address updates. Beyond public CAs, every organization managing its own PKI will also need to make the update. This would include notable providers of card-based credentials, such as personal identity verification, the Transportation Worker Identification Credential, and the common access card, all of which store digital certificates (DHS, 2009). Every organization’s or individual’s active digital certificate will likely need to be reissued. Other organizations in the identity management ecosystem would include the Social Security Administration, state departments of motor vehicles, U.S. Customs and Border Protection, the Transporta-
tion Security Administration, U.S. Citizenship and Immigration Services, the U.S. Postal Service, providers in counties and municipalities, and private-sector identity management services (Better Identity Coalition, 2018). All of these organizations would need to address updates of some kind.

Cost
Our assessment is that cost per organization for this NCF is low. The cost for the NCF as a whole might be substantial, involving considerable effort from commercial and private CAs to reissue certificates, but that cost is likely to be borne by many individual organizations over a long timeline. Many organizations will likely need to pay to have a certificate reissued only after a new standard is implemented. Because certificates need to use PQC only before a CRQC arrives, even organizations managing their own PKI might incur low costs by allowing certificates to be reissued for their users along routine revocation and renewal timelines after a new standard is adopted.

Other Factors
Our assessment is that other factors for this NCF are mitigating. The high degree of standardization and interoperability among systems that use digital certificates is likely to significantly ease the transition to a post-quantum digital certificate. Organizations in this NCF have been collaborating on solutions to these issues for some time, and it is likely that standards for post-quantum and hybrid authentication mechanisms will be ready very quickly after the completion of the NIST PQC standardization project (Entrust, undated). This is a strong mitigating factor.

Priority for Assistance
We rated the NCF as a medium priority for assistance. Although the scope is high, organizations have time to address vulnerabilities, and there is evidence of significant collaboration within the NCF to have solutions ready when a PQC standard is finalized.

References
Works That Informed the Analysis
DHS, Information Technology Sector Baseline Risk Assessment, August 2009.
Mozilla, “Common CA Database,” webpage, undated.

National Critical Function 36, Provide Insurance Services

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>This national critical function (NCF) handles sensitive personal and proprietary business data that could have a moderate confidentiality lifetime.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other NCFs. Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>The importance of systemic cyber-risks to various insurance lines of business might incentivize a broader awareness of relevant issues in this NCF.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in most categories lead to a rating of low priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>Organizations in the NCF should begin early preparations for the post-quantum cryptography (PQC) migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Operate systems and markets to transfer financial risks among parties through contractual relationships, including products for individuals, corporations, and public-sector entities” (CISA, 2020b, p. 5).

Synopsis of Issues

The NCF will experience moderate catch-and-exploit vulnerabilities. The NCF handles some sensitive data used to inform assessments of financial risks. Although the sensitivity and protection of some of these categories of data are more appropriately addressed in assessments for other NCFs (e.g., protected health information [PHI] associated with health insurance is discussed with the assessment for NCF 23, Maintain Access to Medical Records), the NCF does occasionally handle proprietary business information that could have a moderate confidentiality lifetime. These data will present catch-and-exploit vulnerabilities until PQC is used to secure data in transit.

This NCF will experience authentication vulnerabilities in products and services provided by other NCFs, and it will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. These vulnerabilities arise from the ubiquitous use of public-key cryptography to identify and authenticate users and equipment across the Internet. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer arrives.1

---

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business information technology (IT) systems. We assessed that this group included NCFs 20, 21, 26, 27, 31, 36, and 51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.
Urgency
Our assessment is that urgency of action for this NCF is medium. The NCF handles sensitive personal and proprietary business data that could have a moderate confidentiality lifetime. Transmissions of these data will need to adopt PQC soon after the standard is released. Internet-dependent business IT products and services will also need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for providing updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. Quantum computing vulnerabilities present a source of systemic risk that will affect various insurance lines of business. Many of the larger insurance providers are therefore likely to stay apprised of relevant quantum computing vulnerabilities because those vulnerabilities will inform their risk analyses for customers and present a potential business opportunity (Zardoshti, 2021). This incentive to stay apprised of the business risks could translate to better internal cybersecurity risk management, and it is assessed as a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings, on average, in assessed factors.

References
Works That Informed the Analysis
National Critical Function 37, Provide Medical Care

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
</tr>
</tbody>
</table>

Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.

Situations requiring active, swift risk mitigation are likely to be rare.

Mitigation is likely to take place mostly through software updates and in-cycle hardware replacement.

We identified no mitigating or exacerbating factors.

Low ratings in all categories except cost lead to a rating of low priority for assistance.

Protected health information (PHI) is vulnerable to catch and exploit with a long confidentiality lifetime but is covered under other national critical functions (NCFs). Medical research and development (R&D) intellectual property (IP), which also has a long confidentiality lifetime, is also vulnerable to catch and exploit but is covered under other NCFs.

CISA definition: “Ensure the provision of healthcare services” (CISA, 2020b, p. 5).

Synopsis of Issues

We identified two major catch-and-exploit issues: (1) the transmission of PHI between medical facilities and (2) the transmission of sensitive IP for medical R&D (expecting that, over time, the degradation of medical R&D would eventually degrade the quality of medical care). Both of these vulnerabilities are discussed in more detail with assessments for other NCFs: The transmission of PHI is covered in the assessment of NCF 23, Maintain Access to Medical Records, and the transmission of medical R&D is covered with the assessment of NCF 54, Research and Development. Any transmissions involving medical care that do not contain any patient PHI or R&D IP results are unlikely to have a long confidentiality lifetime.

Authentication vulnerabilities (excluding PHI and R&D IP) will be present in networked information technology products and services used to support operations. Failure to maintain effective authentication for network access (e.g., in cloud-based services and applications for communication, remote network access, and enterprise resource management) and would lead to the general disruption of medical operations (e.g., by locking authorized users out of electronic medical systems). Failure to secure connected cyber-physical systems would risk inappropriate access to medical devices (e.g., an unauthorized change in the settings of a remotely controlled surgical robot or implanted medical device). These issues stem from the use of public-key infrastructures that will be vulnerable to an attacker with a capable quantum computer, and many relate to products and services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Although these issues are very serious, they need to be addressed only before the arrival of a cryptographically relevant quantum computer.

Urgency

Our assessment is that urgency of action for this NCF is low (excluding issues discussed in the assessments of other NCFs). Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only prior to the arrival of a cryptographically relevant quantum computer. Organizations should nevertheless
begin early preparations for the post-quantum cryptography (PQC) migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, most organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement. Certain specialized medical devices might require more-complex hardware changes, but these need to be addressed only before a capable quantum computer arrives.

**Other Factors**
Our assessment is that other factors for this NCF are neutral. The use of implantable medical devices (IMDs) presents a unique issue for this NCF. These devices have unusually high requirements for power, efficiency, reliability, and long operating lifetime, given the difficulty of removing an IMD from a patient’s body for maintenance. Today’s IMDs rarely use encryption because it would increase power consumption (Best, 2020), but some experts consider this to be a serious security vulnerability in need of correction, so encryption of IMDs might become more common in the near future (Downey, 2019). Device manufacturers will eventually need to ensure that all IMDs use quantum-resistant encryption for security.

**Priority for Assistance**
We rated the NCF as a low priority for assistance (excluding issues covered in discussions of other NCFs) because the low urgency and scope offsetting the moderate costs that a few producers of specialized medical devices might incur.

**References**

*Works That Informed the Analysis*
National Critical Function 38, Provide Payment, Clearing, and Settlement Services

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Summary</th>
<th>Authentication vulnerabilities must be addressed before the arrival of a cryptographically relevant quantum computer (CRQC).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Authentication vulnerabilities must be addressed before the arrival of a cryptographically relevant quantum computer (CRQC).</td>
</tr>
<tr>
<td>Cost</td>
<td>Updates could involve significant software development and limited out-of-cycle hardware replacement for payment service providers.</td>
</tr>
<tr>
<td>Other factors</td>
<td>The federal government jointly operates one important network with a company over which it has enhanced regulatory authority, so it can directly promote a transition to post-quantum cryptography (PQC) on that network.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>We rated this as medium priority because of some transmitted personally identifiable information (PII) with a medium-length confidentiality lifetime and multiple systems that will need to be upgraded, though this is offset by the difficulty of a catch-and-exploit campaign and the presence of existing regulatory and standard-setting structures.</td>
</tr>
</tbody>
</table>

CISA definition: “Carry out processes required for the exchange of assets, including payment (transfer of funds between or among participants), clearing (transmitting, reconciling, and confirming transactions prior to settlement), and settlement (transfer of ownership and payments)” (CISA, 2020b, p. 5).

Synopsis of Issues

The system of online payments is extremely complex and involves activity at many different levels. The largest transactions occur directly between financial institutions and can transfer tens of millions of dollars each. We discuss the encryption issues around these large payments between financial institutions in our discussion of NCF 40, Provide Wholesale Funding. In this discussion, we focus on smaller transactions between end users, such as point-of-sale payments and online payments. Although online payments are often initiated by end users, we focus here on the security of the transactions between financial institutions because the security of the account holders’ online endpoint authentication falls under the scope of the Connect NCFs.

The NCF is unlikely to experience significant catch-and-exploit vulnerabilities. Encrypted payment data in transit is sensitive for two reasons:

- The first concerns theft: A threat actor could intercept a payer’s financial authentication data (such as a credit card number or a bank account number) and generate unauthorized transfers from the payer’s account.
- The second concerns privacy: Payers and recipients might want to keep private the identities of the entities with which they are exchanging payments. This is likely to have a very short confidentiality lifetime.

Information about electronic payment recipients’ identities could remain sensitive for longer periods, but a catch-and-exploit campaign targeting these data would be unlikely to significantly degrade the NCF.
Like other NCFs pertaining to the financial service sector, this NCF will exhibit severe authentication vulnerabilities. The finance sector is a highly interconnected ecosystem of various financial institutions, markets, exchanges, and third-party service providers. The use of public-key cryptography to facilitate remote access to financial services (including authentication of financial transactions) is commonplace in the financial sector (Deodoro et al., 2021; Federal Financial Institutions Examination Council [FFIEC], 2016). A threat actor in possession of a quantum computer could forge digital signatures or digital certificates and initiate counterfeit transactions of various financial assets to either steal those assets or manipulate markets. This vulnerability also applies to accounts that hold blockchain-based tokens (i.e., cryptocurrencies). Although most blockchain-mining processes involving hashing and are not vulnerable to quantum computing (via Shor’s algorithm), transfers of tokens are usually secured with public-key cryptography. So a threat actor with a CRQC would not necessarily be able to directly mine a significant number of tokens, but it would be able to transfer other people’s tokens to its own account (Fedorov, Kiktenko, and Lvovsky, 2018). A threat actor could also exploit vulnerabilities to attain remote access to the internal networks of financial institutions. Even if these vulnerabilities were only rarely exploited, a few well-publicized incidents could greatly shake investor confidence in the reliability of payment, clearing, and settlement services, potentially degrading the functioning of the entire market (Eisenbach, Kovner, and Lee, 2021; Healey et al., 2018). These vulnerabilities need to be addressed only before a CRQC is available.

**Urgency**

Our assessment is that urgency of action for this NCF is low. Encrypted data in motion about electronic payments (both the financial authentication data and senders’ and recipients’ identities) will either have a short confidentiality lifetime or be unlikely to lead to a significant degradation of the function if they were the target of a catch-and-exploit campaign. Authentication vulnerabilities must be addressed merely before the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is high. The five major credit card companies that make up the Payment Card Industry (PCI) Security Standards Council will need to update the PCI data security standard (DSS) to require PQC. The U.S. automated clearinghouse (ACH) network is operated by only two organizations, the Federal Reserve Banks and the Electronic Payments Network, which will need to update their cryptographic systems to PQC throughout the ACH network. After new standards have been implemented, vendors of credit card readers and third-party providers of payment products and services will need to adopt the new standards. This will likely affect thousands of third-party providers (FactSet, 2021).

**Cost**

Our assessment is that cost per organization for this NCF is medium. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. After updated standards are created that implement PQC for transactions, vendors of information technology products and services that facilitate transactions will need to incorporate those standards in software and hardware. Because of the highly interconnected and complex nature of the payment system, this could involve custom software development by financial institutions and third-party service providers and, potentially, off-cycle hardware replacement. The low urgency of

1 The authentication vulnerabilities described here are largely shared by each of the NCFs connected to the financial sector: NCFs 32, 33, 34, 38, and 40.
this effort should, however, allow the migration to happen without the more-extensive software development and off-cycle hardware replacement that would lead to a rating of high cost.²

Other Factors

Our assessment is that other factors for this NCF are mitigating overall, with both mitigating and exacerbating factors present. The NCF might be able to facilitate a fast, robust migration to PQC thanks to significant centralized standard-setting bodies and regulatory authority governing member organizations:

- Many direct (non–credit card) transfers between bank checking or savings accounts (including payroll, social security, vendor, mortgage, utility, and tax payments) occur over ACH or similar networks. In the United States, the ACH network is operated by the Federal Reserve Banks and the Electronic Payments Network, which is operated by the Clearing House Payments Company (Board of Governors of the Federal Reserve System, 2020).³ Because it is crucial to the functioning of the U.S. financial system, the Financial Stability Oversight Council has designated the Clearing House as a systemically important financial market utility under Title VIII of the Dodd–Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111-203, 2010), which places it under enhanced regulatory scrutiny (Board of Governors of the Federal Reserve System, 2015). Moreover, some U.S. federal organizations, such as the FFIEC, promote cybersecurity best practices in the financial sector, including resources focusing specifically on network authentication and access (FFIEC, 2021). The goal of the FFIEC is to ensure uniformity in the supervision of financial institutions, thereby improving regulatory coordination that could promote a successful industry transition to PQC.

- The security of most online credit card payments is managed by the PCI DSS, which is managed by the PCI Security Standards Council (PCI Security Standards Council, 2010). One requirement of the PCI DSS is that organizations that handle credit card payments encrypt the transmission of cardholder data over open networks.

The financial sector has also been notably aware of the issues created by quantum computing and proactive in preparing for the migration to PQC (Castellanos, 2020; Eisenbach, Kovner, and Lee, 2021; Toshiba Corporation, 2020). We assessed these to be mitigating factors.

However, the potential ability to directly steal financial assets is likely to make financial institutions high-value targets for most potential threat actors. Banking is often the industry most affected by cybercrime (Bissell, LaSalle, and Dal Cin, 2019). Although impersonation attacks that allow counterfeit transactions are an authentication vulnerability that needs to be addressed only just before a CRQC is available, it is likely that such attacks would be among the first attempted by an attacker with the capability to do so. There is therefore likely to be little room for delay in the migration to PQC in the financial sector. Furthermore, the interconnected nature of the financial system and the shared technological vulnerability from quantum computing make it likely that even a rare successful attack could lead to systemic shocks that could significantly degrade the function (Eisenbach, Kovner, and Lee, 2021). We assessed these to be exacerbating factors.

² Like with many other assessments, we assumed that information technology products and services that enable the migration to PQC will be available quickly after the completion of the National Institute of Standards and Technology’s PQC standardization project and that organizations can therefore wait until the planned end of life of hardware to replace it with a PQC-compatible version. In case this assumption does not hold true, Petrenko, Mashatan, and Shirazi, 2019, provides a detailed estimate of the high cost for a large financial institution to perform an off-cycle hardware migration to accommodate PQC.

³ The volume of ACH transfers has increased significantly since the Federal Reserve Board enhanced same-day ACH service in 2019.
Priority for Assistance
We rated the NCF as a medium priority for assistance. Although urgency is low, many organizations will be affected, and costs to address vulnerabilities might not be trivial for affected organizations. Migration to PQC might be facilitated by the relatively centralized regulatory and standard-setting authority affecting the NCF, but NCF organizations are also likely to be high-priority targets.

References
Works That Informed the Analysis
FactSet, financial data and analytics, 2021.
Related Reading
National Critical Function 39, Provide Public Safety

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Low</th>
<th>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs) or without active intervention. Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>The NCF’s strong support from federal and private organizations and the reliance on open standards in wireless communications.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Organizations in the NCF should ensure that wireless communication systems being implemented now are forward compatible with expected updates to communication standards. Organizations in the NCF should begin early preparations for the post-quantum cryptography (PQC) migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Provide public services—to include police, fire, and emergency medical services—to ensure the safety and security of communities, businesses and populations” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted. Any overlap with sensitive law enforcement or medical record data is addressed in more detail in the discussions of our assessments of NCFs 22, Enforce Law, and 23, Maintain Access to Medical Records, respectively, and is not considered here.

Few authentication vulnerabilities exist in the communication architectures for public safety, as currently constructed, although future generations might need to address additional vulnerabilities.¹ Communications are a combination of legacy land mobile radio and modernized wireless broadband communication systems, such as the Nationwide Public Safety Broadband Network (CISA, 2019a). Wireless communication devices typically rely on preshared or embedded symmetric keys for security (where encryption is used at all), and these communications are therefore already inherently quantum resistant.² Future public safety communication networks are expected to prioritize interoperability and rely on open standards for implementation (Parkinson, 2020). Some security mechanisms, especially those used in fifth-generation (5G) networks, use public key–based authentication to identify user equipment, and these will present an authentication vulnerability until they adopt PQC (Mitchell, 2020). The Nationwide Public Safety Broadband Network, specifically, allows the use of public-key infrastructure in client security management (Local Control Working Group, 2015), and this would present an authentication vulnerability until it is updated with post-quantum

¹ There is significant overlap between the communication systems used for provision of public safety and those used for emergency response, so this assessment shares many similarities with that for NCF 39, Provide Public Safety.

² Many of the issues associated with wireless broadband networks are discussed in more detail in the discussion of our assessment of NCF 8, Provide Wireless Access Network Services.
protocols. Like many other organizations, public safety organizations will face authentication vulnerabilities in networked information technology systems, and they will depend on other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services) to provide relevant updates to those products and services.

**Urgency**
Our assessment is that urgency of action for this NCF is low. The use of symmetric-key cryptography in wireless broadband network communications provides a measure of quantum resistance, even where weak symmetric keys are used. Parts of those networks that use public-key infrastructure to authenticate users will need to migrate to a new standard for digital certificates and signatures. Internet-dependent business information technology products and services will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**
Our assessment is that scope for this NCF is low because the most-affected products and services for wireless communications have a degree of inherent quantum-resistant security, and public safety organizations can likely allow them to be replaced with long-term secure solutions through normal hardware obsolescence and replacement cycles. Most other affected products and services are provided by other NCFs, and those NCFs will be responsible for providing updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**
Our assessment is that other factors for this NCF are mitigating. The reliance on open standards in the architectures of future wireless broadband communication networks for public safety make it likely that relevant systems will have the forward compatibility and necessary organizational support to adapt when those standards are updated for quantum-resistant solutions. The NCF is also strongly supported by federal coordinating bodies and public–private partnerships on public safety communication systems (CISA, 2019a). We assessed these to be mitigating factors.

**Priority for Assistance**
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

**References**
Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.

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.


Related Reading

CISA, "Emergency Communications," webpage, undated a.
National Critical Function 40, Provide Wholesale Funding

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Situations requiring active, swift mitigation are likely to be rare. Moreover, the provision of services for this national critical function (NCF) is concentrated in just two large networks, so a limited number of organizations need to take action.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Migration is likely to take place through routine, conventional cybersecurity efforts, such as software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>The federal government either directly operates the key systems or has unusually strong regulatory control over the companies that operate them, so it can directly promote a transition to post-quantum cryptography (PQC). The financial sector is a likely target, however, and even rare attacks could cause systemic disruption.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

After the arrival of a cryptographically relevant quantum computer (CRQC), authentication vulnerabilities will be unusually severe because of the huge volume of financial transactions handled by this NCF. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Maintain processes for lending and borrowing among financial services sector parties” (CISA, 2020b, p. 6).

Synopsis of Issues

The U.S. financial sector uses a variety of systems for transferring funds electronically between financial institutions. The two most-important systems for transfers between domestic financial institutions are the Fedwire Funds Service, which is operated by the U.S. Federal Reserve Banks, and the Clearing House Interbank Payments System (CHIPS), which is privately owned by the Clearing House, which is jointly owned by 24 large commercial banks that use CHIPS.¹ Almost all domestic payments between financial institutions use one of these two systems (Smith and Moolji, 2017). These systems handle an enormous amount of money: Fedwire and CHIPS transferred around $840 trillion and $657 trillion in 2021, respectively (Clearing House, undated; Federal Reserve Banks, undated). Because it is crucial to the functioning of the financial system, the Financial Stability Oversight Council has designated the Clearing House as a systemically important financial market utility under Title VIII of the Dodd–Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111-203, 2010), which places the entity under enhanced regulatory scrutiny (Board of Governors of the Federal Reserve System, 2015).

Most low-value interbank transfers, such as payments between individuals, are conducted via the automated clearinghouse (ACH) network, which is operated by the Federal Reserve Banks and the Electronic

¹ Fedwire is a real-time gross settlement system, meaning that all transactions are settled (i.e., finalized) as soon as they are processed. CHIPS is a net settlement system, meaning that credits and debits between two institutions are recorded but not immediately settled, and the net of all credits and debits are settled periodically. Fedwire transfers are settled faster but incur higher transfer fees, so which system is used depends on the urgency of the transfer. Fedwire has a much broader network, with approximately 7,300 participants in 2008 (versus approximately 50 for CHIPS in 2021) (Board of Governors of the Federal Reserve System, 2021; Clearing House, undated).
Preparing for Post-Quantum Critical Infrastructure

Payments Network, which is operated by the Clearing House (Board of Governors of the Federal Reserve System, 2020). Most international financial transfers from U.S. banks use the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network to send payment orders between countries (SWIFT, undated). The funds are then transferred over Fedwire, CHIPS, or a similar system. These networks rely on public-key infrastructures and digital certificates to authenticate users and transactions (Federal Financial Institutions Examination Council [FFIEC], 2021; SWIFT, 2021).

The primary data in transit regarding lending and borrowing within the financial service sector concerns requests for transfers and the direct transfers of funds, which take place using the networks described above. Our assessment is that none of these data contains personally identifiable information (PII) or has a long confidentiality lifetime, so we identified no catch-and-exploit vulnerabilities.

Like other NCFs pertaining to the financial service sector, this NCF will exhibit severe authentication vulnerabilities. The finance sector is a highly interconnected ecosystem of various financial institutions, markets, exchanges, and third-party service providers. The use of public-key cryptography to facilitate remote access to financial services (including authentication of financial transactions) is commonplace in the financial sector (Deodoro et al., 2021; FFIEC, 2016). A threat actor in possession of a quantum computer could forge digital signatures or digital certificates and initiate counterfeit transactions of various financial assets to either steal those assets or manipulate markets. Such an actor could also exploit vulnerabilities to achieve remote access to the internal networks of financial institutions. Although, for this NCF, the set of possible recipients of fraudulent transactions would be limited to the other members of the Fedwire or CHIPS networks, given the huge volume of funds passing through these networks, even a rare authentication vulnerability could lead to a large amount of money being misdirected. This has the potential to significantly degrade the functioning of the NCF by harming user confidence in the transaction systems (Eisenbach, Kovner, and Lee, 2021; Healey et al., 2018). These vulnerabilities need to be addressed only before a CRQC is available.

Urgency

Our assessment is that urgency of action for this NCF is low. Although it will be critical to adopt PQC to prevent falsified authentication into the network, this needs to be completed only before the arrival of a CRQC. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope

Our assessment is that scope for this NCF is low. Almost all electronic fund transfers between U.S. financial institutions are conducted over just two networks, Fedwire and CHIPS (with a third network, SWIFT, being used for most international transfers). If the two organizations operating these networks ensure that their systems transition to PQC, the vast majority of lending between financial institutions will be secure.

---

2 The ACH system processes many (typically fairly small) payments together in batches. As a result, it has low fees but has historically been slow and relatively little used. In 2019, the Board of Governors of the Federal Reserve System enhanced same-day ACH service, which has caused the volume of ACH transfers to increase significantly, although it still represents a small fraction of the value of Fedwire and CHIPS transfers (Board of Governors of the Federal Reserve System, 2020).

3 The authentication vulnerabilities described here are largely shared by each of the NCFs connected to the financial sector: NCFs 32, 33, 34, 38, and 40.
Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the
preparation steps outlined in the DHS roadmap. The primary networks must adopt a new standard for digital
certificates in post-quantum public-key infrastructures. Other efforts to migrate to PQC are likely to take
place as part of routine, conventional cybersecurity efforts, such as software updates, security patches, and
in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are neutral, with mitigating and exacerbating factors pres-
ent. The federal government has a greater ability to directly speed up the adoption of PQC in the financial
sector than in many other NCFs because it already closely regulates the financial sector. One of the two
most-important networks for this NCF is directly operated by a federal agency (the Federal Reserve), and the
other one is operated by a company over which the government has enhanced regulatory authority under the
Dodd–Frank Wall Street Reform and Consumer Protection Act. Moreover, some U.S. federal organizations,
such as the FFIEC, that promote cybersecurity best practices in the financial sector, including resources
focusing specifically on network authentication and access (FFIEC, 2021). The goal of the FFIEC is to ensure
uniformity in the supervision of financial institutions, thereby improving regulatory coordination that could
promote a successful industry transition to PQC. The financial sector has also been notably aware of the
issues created by quantum computing and proactive in preparing for the migration to PQC (Castellanos,
2020; Eisenbach, Kovner, and Lee, 2021; Toshiba Corporation, 2020). We assessed these to be mitigating
factors.

The potential ability to directly steal financial assets is likely to make financial institutions high-value
targets for most potential threat actors. Banking is often the industry most affected by cybercrime (Biss-
sell, LaSalle, and Dal Cin, 2019). Although impersonation attacks that allow counterfeit transactions are an
authentication vulnerability that needs to be addressed only just before a CRQC is available, it is likely that
such attacks would be among the first attempted by an attacker with the capability to do so. Therefore, there
is likely to be little room for delay in the migration to PQC in the financial sector. Furthermore, the intercon-
nected nature of the financial system and the shared technological vulnerability from quantum computing
make it likely that even a rare successful attack could lead to systemic shocks that could significantly degrade
the function (Eisenbach, Kovner, and Lee, 2021). We assessed these to be exacerbating factors.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all categories.

References
Works That Informed the Analysis
Bissell, Kelly, Ryan M. LaSalle, and Paolo Dal Cin, The Cost of Cybercrime: Ninth Annual Cost of Cybercrime
Study, Accenture, March 6, 2019.

Board of Governors of the Federal Reserve System, "Designated Financial Market Utilities,” webpage, last


Castellanos, Sara, “Visa, JPMorgan Are Already Preparing for Potential Quantum Cyberattacks,” Wall Street

Preparation for Post-Quantum Critical Infrastructure


Related Reading
National Critical Function 41, Store Fuel and Maintain Reserves

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
</tr>
<tr>
<td>Scope</td>
</tr>
<tr>
<td>Cost</td>
</tr>
<tr>
<td>Other factors</td>
</tr>
<tr>
<td>Priority for assistance</td>
</tr>
</tbody>
</table>

Primary concern(s)

Organizational network access and systems that secure ICSs must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Store energetic materials (including fossil and nuclear fuels) to reliably meet operational and strategic demands” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

The NCF will experience authentication vulnerabilities in information technology (IT) systems and cyber-physical systems. The NCF consists of a diverse group of stakeholders, owners, and operators that use a complex mix of aging and modern communication, control, and distribution systems (Nygaard and Mukhopadyay, 2020). Internet-based communication systems are increasingly used to improve interoperability and cybersecurity (Stouffer et al., 2015), and these will present quantum computing vulnerabilities in authentication where they are used. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography-based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of

1 The oil and natural gas (ONG) supply chain (described in Nygaard and Mukhopadyay, 2020) integrates elements from NCF 17, Transport Materials by Pipeline; NCF 41, Store Fuel and Maintain Reserves; NCF 43, Exploration and Extraction of Fuels; and NCF 44, Fuel Refining and Processing Fuels. As a result, the assessments for the NCFs address many of the same organizations, IT and operational technology systems, and vulnerabilities, and their content is very similar.
these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.2

Urgency
Our assessment is that urgency of action for this NCF is low. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and in-cycle hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low. Although the ONG industry alone includes thousands of organizations and stakeholders (FactSet, 2021), most will not need to take significant action that specifically addresses quantum computing vulnerabilities, and they are therefore not included in the scope. Each stakeholder will need to consider how quantum computing vulnerabilities need to be integrated into broader cybersecurity risk management and associated IT and operational technology acquisition strategy. Most affected products and services are provided by other NCFs, however, and those NCFs will likely provide the required updates.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. Mitigation is likely to take place through configuration changes, software updates, security patches, and in-cycle hardware replacement for affected technologies. Where vulnerabilities remain that are not addressed by those actions, the industry’s ongoing adoption of defense-in-depth strategies in ICSs is likely to be adequate for risk reduction related to quantum computing (ONG Subsector Coordinating Council, 2018).

Other Factors
Our assessment is that other factors for this NCF are exacerbating on balance, with mitigating and exacerbating factors present. The ONG industry increasingly integrates legacy operational technology and IT with modern automated, connected systems in order to improve productivity, but the industry as a whole has not adequately prioritized cybersecurity. Moreover, the industry has not exhibited effective coordination with federal partners on cybersecurity (especially ICS security) incident prevention and management, although this has been improving in recent years. Regulation and standardization in the industry are also complex:

[T]he sheer number of differing regulatory bodies and trade groups offering both standards and best-practice recommendations for oil and natural gas (ONG) cybersecurity makes it difficult to create a com-

---

2 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
prehensive, directed, and coherent strategy that is applicable to all players within the ONG industry. (Nygaard and Mukhopadyay, 2020, p. iii)

Together, these factors indicate a strong possibility that the NCF will not respond to risks from quantum computing vulnerabilities in a robust, coordinated, and timely manner, and this is assessed as a significant exacerbating factor.

Deployed ICS technology is often resource-constrained, and 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). Networked ICSs often also rely on additional, redundant 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; ONG Subsector Coordinating Council, 2018). This is assessed as a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

References
Works That Informed the Analysis
FactSet, financial data and analytics, 2021.
National Critical Function 42, Support Community Health

Category: Manage

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Medium</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Medium</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>PHI has an extremely long confidentiality lifetime that (under current law) extends even beyond a patient’s death. Electronic laboratory reporting mechanisms should implement PQC in key exchange to protect against catch-and-exploit vulnerabilities.</td>
</tr>
</tbody>
</table>

This national critical function (NCF) handles a significant amount of protected health information (PHI) with a confidentiality lifetime of many decades.

A small number of major vendors will need to push out software updates to their customers.

Mitigation is likely to take place through software updates and in-cycle hardware replacement for most organizations.

Significant standardization and interoperability in the NCF will help facilitate the migration to post-quantum cryptography (PQC); threat actors with sufficient resources for a catch-and-exploit campaign are unlikely to target PHI.

The NCF has high urgency because of the very long confidentiality lifetime of PHI, but the risk is diminished by the limited number of organizations that need to take proactive action and the low cost of doing so.

CISA definition: “Conduct epidemiologic surveillance, environmental health, migrant and shelter operations, food establishment inspections, and other community-based public health activities” (CISA, 2020b, p. 6).

Synopsis of Issues

This NCF exhibits serious catch-and-exploit vulnerabilities. Epidemiologic surveillance involves the handling of PHI, which remains legally protected not only throughout a patient’s entire lifetime but for 50 years after their death (Office for Civil Rights, 2013), so, under current law, some PHI being generated today could remain sensitive for well over a century. Epidemiologic surveillance routinely involves the collection and management of PHI from field investigations, along with a variety of other data required by field investigators, and those functions are often facilitated by Internet-based information technology products and services (e.g., cloud-based services or mobile applications) (Hamilton and Hopkins, 2019). Reportable health information is also often transmitted electronically from laboratory information management systems (LIMS) or medical provider electronic health record (EHR) systems to public health organizations in standardized formats (e.g., Health Level Seven [HL7] version 2.5.1), and these messages depend on other Internet protocol–based encryption mechanisms for security (Centers for Disease Control and Prevention [CDC], 2021; Google Cloud, 2021). These products and services rely on vulnerable public-key cryptography for secure communications, and they present a significant catch-and-exploit vulnerability until the migration to use PQC in key exchange.

Authentication vulnerabilities in the NCF relate to administrators’ and field investigators’ reliance on Internet-based services in their operations, including in remote access to their internal networks. There are also authentication issues for LIMSS and databases containing PHI, which are ubiquitous in medical facilities of all kinds. Several major cyberattacks on PHI databases might already have exposed the medical records of tens of millions of people (Snell, 2015a; Snell, 2015b). A hostile actor who gains access to these databases could

---

1 The issues affecting this NCF substantially overlap with those affecting NCF 23, Maintain Access to Medical Records. As a result, the content and conclusions in these assessments are very similar.
acquire PHI at rest (with the negative consequences described above) or even modify, corrupt, or destroy it. The NCF requires assured remote access and fidelity of these databases, each of which will require updates to protocols used for secure remote access over the Internet before an attacker possesses a capable quantum computer.

**Urgency**

Our assessment is that urgency of action for this NCF is high. The exceptionally long confidentiality lifetime of PHI (often well over 100 years) means that it is very likely that a cryptographically relevant quantum computer will be developed while PHI being generated today still remains sensitive. The sooner that products and services used by field investigators to collect and transmit PHI adopt PQC in key exchange, the less stored data will be vulnerable for decryption. Updating the security protocols for remote access to PHI databases and internal networks is a just-in-time risk that is much lower urgency. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the U.S. Department of Homeland Security (DHS) roadmap.

**Scope**

Our assessment is that scope for this NCF is medium. Although thousands of laboratories, health care providers, and state and federal public health agencies participate in the sharing of data in support of community health, the primary responsibility for addressing vulnerabilities will likely fall on a relatively small number (between ten and 100) of providers of software products and services that facilitate data-sharing, including LIMS software, EHR software, and other mobile software that supports data management in field investigations (FactSet, 2021; “LIMS Vendor,” 2021). These providers will need to make software and configuration changes in their products, which will be pushed out to their customers. Other vulnerabilities associated with use of the Internet to access and deliver data are the responsibility of other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services).

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. Most required actions can be achieved through software updates pushed out by vendors. These updates would likely involve a relatively low level of software development effort for vendors (e.g., incorporating a new standard algorithm for key exchange), and laboratories, health care providers, and public health organizations would need only to implement these updates. Moreover, medical records are generally transmitted between commercial off-the-shelf computer systems that are replaced at regular cycles.

**Other Factors**

Our assessment is that other factors for this NCF are, on balance, mitigating. Several national and international organizations develop interoperability standards and specifications for the medical industry, such as the Center for Medical Interoperability and HL7, which maintains the internationally used HL7 standard for medical data. These organizations will be useful in efforts to disseminate information, guidance, and other resources to others in the NCF.

Depending on their motivations, threat actors could attempt either bulk collection of PHI or targeted collection of a specific person’s PHI. A large-scale catch-and-exploit campaign would involve significant practical challenges. A threat actor would likely not know what data were in a bulk capture of data until it actually decrypted the many communication streams. The significant resource requirements needed to do
this decryption, combined with the likely low utility of the desired PHI data, would make such a bulk catch- and-exploit campaign unlikely for a realistic threat actor. It might be difficult for even a high-resource threat actor to predict whose medical data will be useful ten or more years in the future, then capture communications specifically concerning them. We assess that these considerations significantly mitigate the threat of a catch-and-exploit campaign targeting PHI.

Priority for Assistance
We rated the NCF as a medium priority for assistance because of the exceptionally long confidentiality lifetime of PHI, offset by the relatively small number of major software vendors that need to update products and services to enable the use of PQC.

References
Works That Informed the Analysis
CDC, “Standards to Facilitate Data Sharing,” webpage, last reviewed March 5, 2014.
———, “How Does ELR Work?” webpage, last reviewed April 6, 2021.
FactSet, financial data and analytics, 2021.
“LIMS Vendor,” LIMSWiki, October 6, 2021.
National Critical Function 43, Exploration and Extraction of Fuels

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, but long-lived operational technology could embed vulnerabilities for long durations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
<td>The NCF is operationally complex, has historically not prioritized cybersecurity, and lacks a common approach to standardization and cybersecurity. Layered security in industrial control system (ICS) networks could mitigate some vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
</tbody>
</table>

Primary concern(s)

Within a few years of the release of the PQC standard, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets. Organizational network access and systems that secure ICS must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Identify resources and collect energetic materials (including fossil fuels, nuclear materials, and others)” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF could experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit (Oil and Natural Gas [ONG] Subsector Coordinating Council, 2018). It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to PQC in communications is delayed.

The NCF will experience authentication vulnerabilities in information technology (IT) systems and cyber-physical systems. The NCF consists of a diverse group of stakeholders, owners, and operators that use a complex mix of aging and modern communication, control, and distribution systems (Nygård and Mukhopadyay, 2020). Internet-based communication systems are increasingly used to improve interoperability and cybersecurity (Stouffer et al., 2015), and these will present quantum computing vulnerabilities in

---

1 The ONG supply chain (described in Nygaard and Mukhopadyay, 2020) integrates elements from NCF 17, Transport Materials by Pipeline; NCF 41, Store Fuel and Maintain Reserves; NCF 43, Exploration and Extraction of Fuels; and NCF 44, Fuel Refining and Processing Fuels. As a result, the assessments for the NCFs address many of the same organizations, IT and operational technology systems, and vulnerabilities, and their content is very similar.
authentication where they are used. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.²

Urgency
Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Nevertheless, operational hardware used by the NCF has a long operational lifetime, and hardware installed now could be embedding hard-to-update vulnerabilities into infrastructure until quantum resistance is incorporated into industry cybersecurity risk management. Organizations should begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low. Although the ONG industry alone includes thousands of different organizations and stakeholders (FactSet, 2021), most will not need to take significant action that specifically addresses quantum computing vulnerabilities, and they are therefore not included in the scope. Each stakeholder will need to consider how quantum computing vulnerabilities need to be integrated into broader cybersecurity risk management and associated IT and operational technology acquisition strategy. Most affected products and services are provided by other NCFs, however, and those NCFs will likely provide the required updates.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement. Where vulnerabilities remain that are not addressed by those actions, the industry’s ongoing adoption of defense-in-depth strate-

² This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

Other Factors
Our assessment is that other factors for this NCF are exacerbating on balance, with mitigating and exacerbating factors present. The ONG industry increasingly integrates legacy operational technology and IT with modern automated, connected systems in order to improve productivity, but the industry as a whole has generally not adequately prioritized cybersecurity. Moreover, the industry has not exhibited effective coordination with federal partners on cybersecurity (especially ICS security) incident prevention and management, although this has been improving in recent years. Regulation and standardization in the industry are also complex:

[T]he sheer number of differing regulatory bodies and trade groups offering both standards and best-practice recommendations for oil and natural gas (ONG) cybersecurity makes it difficult to create a comprehensive, directed, and coherent strategy that is applicable to all players within the ONG industry. (Nygaard and Mukhopadyay, 2020, p. iii)

Together, these factors indicate a strong possibility that the NCF will not respond to risks from quantum computing vulnerabilities in a robust, coordinated, and timely manner, and this is assessed as a significant exacerbating factor.

Deployed ICS technology is often resource-constrained, and 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). Networked ICSs often also rely on additional, redundant 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; ONG Subsector Coordinating Council, 2018). This is assessed as a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of low ratings, on average, in assessed factors.

References
Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.
FactSet, financial data and analytics, 2021.

National Critical Function 44, Fuel Refining and Processing Fuels

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, but long-lived operational technology could embed vulnerabilities for long durations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Exacerbating</td>
<td>The NCF is operationally complex, has historically not prioritized cybersecurity, and lacks a common approach to standardization and cybersecurity. Layered security in industrial control system (ICS) networks could mitigate some vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>• Within a few years, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets. • Organizational network access and systems that secure ICSs must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Transform raw energetic materials into consumer fuels (e.g., crude cracking, gas separation, and uranium enrichment)” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF might experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit (Oil and Natural Gas [ONG] Subsector Coordinating Council, 2018). It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to PQC in communications is delayed.

The NCF will experience authentication vulnerabilities in information technology (IT) systems and cyber-physical systems. The NCF consists of a diverse group of stakeholders, owners, and operators that use a complex mix of aging and modern communication, control, and distribution systems (Nygaard and Mukhopadyay, 2020). Internet-based communication systems are increasingly used to improve interoperability and cybersecurity (Stouffer et al., 2015), and these will present quantum computing vulnerabilities in

---

1 The ONG supply chain (described in Nygaard and Mukhopadyay, 2020) integrates elements from NCF 17, Transport Materials by Pipeline; NCF 41, Store Fuel and Maintain Reserves; NCF 43, Exploration and Extraction of Fuels; and NCF 44, Fuel Refining and Processing Fuels. As a result, the assessments for the NCFs address many of the same organizations, IT and operational technology systems, and vulnerabilities, and their content is very similar.
authentication where they are used. Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.2

**Urgency**

Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Nevertheless, operational hardware used by the NCF has a long operational lifetime, and hardware installed now could be embedding hard-to-update vulnerabilities into infrastructure until quantum resistance is incorporated into industry cybersecurity risk management. Organizations should begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is low. Although the ONG industry alone includes thousands of organizations and stakeholders (FactSet, 2021), most will not need to take significant action that specifically addresses quantum computing vulnerabilities, and they are therefore not included in the scope. Each stakeholder will need to consider how quantum computing vulnerabilities need to be integrated into broader cybersecurity risk management and associated IT and operational technology acquisition strategy. Most affected products and services are provided by other NCFs, however, and those NCFs will likely provide the required updates.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement. Where vulnerabilities remain that are not addressed by those actions, the industry’s ongoing adoption of defense-in-depth strate-

---

2 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Assessments of Quantum Computing Vulnerabilities in the National Critical Functions

Other Factors
Our assessment is that other factors for this NCF are exacerbating on balance, with mitigating and exacerbating factors present. The ONG industry increasingly integrates legacy operational technology and IT with modern automated, connected systems in order to improve productivity, but the industry as a whole has generally not adequately prioritized cybersecurity. Moreover, the industry has not exhibited effective coordination with federal partners on cybersecurity (especially ICS security) incident prevention and management, although this has been improving in recent years. Regulation and standardization in the industry are also complex:

"The sheer number of differing regulatory bodies and trade groups offering both standards and best-practice recommendations for oil and natural gas (ONG) cybersecurity makes it difficult to create a comprehensive, directed, and coherent strategy that is applicable to all players within the ONG industry." (Nygaard and Mukhopadyay, 2020, p. iii)

Together, these factors indicate a strong possibility that the NCF will not respond to risks from quantum computing vulnerabilities in a robust, coordinated, and timely manner, and this is assessed as a significant exacerbating factor.

Deployed ICS technology is often resource-constrained, and 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). Networked ICSs often also rely on additional, redundant 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; ONG Subsector Coordinating Council, 2018). This is assessed as a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings, on average, in assessed factors.

References
Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.
FactSet, financial data and analytics, 2021.

National Critical Function 45, Generate Electricity
Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
</tr>
<tr>
<td>Cost</td>
<td>High</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>High</td>
</tr>
</tbody>
</table>

Updates need to happen only before a cryptographically relevant quantum computer (CRQC) is available, but forward compatibility with post-quantum cryptography (PQC) should be incorporated into existing modernization efforts to avoid embedding vulnerability.

Thousands of providers in this national critical function (NCF) will need to address updates of varying kinds.

The operational complexity and heterogeneity of systems and regulations across the United States will lead to high costs as each system independently assesses where and how to incorporate PQC.

The heterogeneity of the NCF could slow adoption of PQC, but ongoing modernization efforts and layered security in industrial control system (ICS) networks could mitigate cost and urgency.

The NCF is a high priority for assistance because of the broad, heterogeneous scope; complex long-range modernization activities; and high expected costs.

Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap, with an emphasis on ensuring forward compatibility with PQC in ongoing modernization efforts.

CISA definition: “Produce electricity from a variety of primary energy sources (including fossil fuels, nuclear materials, and renewables) to reliably meet demand” (CISA, 2020b, p. 6).

Synopsis of Issues

NCF 10, Distribute Electricity; NCF 12, Transmit Electricity; and NCF 45, Generate Electricity, are closely related operationally. To the extent possible, this assessment deals solely with issues at points of electricity generation, although generation operations are significantly affected by the manner in which electricity is transmitted and distributed, especially with respect to the incorporation of distributed generation. These three NCFs share many of the same affected organizations, systems, and vulnerabilities, and the assessments are therefore similar in some respects.

The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

The NCF will experience authentication vulnerabilities in information technology (IT) systems and cyber-physical systems. Electricity has historically been generated at bulk power plants and transmitted through the grid to meet consumer demand, but the industry has been adapting to accommodate the recent increase in distributed energy resources (DERs) and new load balancing challenges (e.g., increases in off-peak demands from charging electric vehicles) (Cleveland and Lee, 2013; Smart Grid Cybersecurity Committee, 2014). Bulk power plants vary widely in the underlying ICSs and IT systems used, but they have relatively few logical interfaces with external systems (compared with other systems for electricity transmission and distribution) (Smart Grid Cybersecurity Committee, 2014; Office of Electricity Delivery and Energy Reliability, 2015). Bulk power generation facilities might experience authentication vulnerabilities where vulnerable cryptography is used in these logical interfaces or for remote access and monitoring of ICSs. DER generation, in contrast, can have a much more complex and varied logical integration with the IT and operational technology of distribution operations, and it often has increased reliance on secured communication technologies (Cleveland and Lee, 2013; Smart Grid Cybersecurity Committee, 2014). DER generation enti-
ties will also experience authentication vulnerabilities, especially where public-key cryptography is used for access control and authentication in ICSs and logical interfaces with electricity distribution systems. Like many other NCFs, this NCF will experience quantum computing vulnerabilities in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management), especially where they are integrated with cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.1

Urgency

Our assessment is that urgency of action for this NCF is medium. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Operational hardware used by the NCF has a long operational lifetime, however, and hardware installed now could be embedding hard-to-update vulnerabilities into infrastructure until quantum resistance is integrated into industry cybersecurity risk management. The NCF might need to act with some urgency to avoid costly retrofits to address vulnerabilities in the future. Organizations should begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope

Our assessment is that scope for this NCF is high. Approximately 3,200 electric utilities provide power to customers in the United States (Office of Electricity Delivery and Energy Reliability, 2015), and a significant portion of them might need to take action of some kind. The growing number of local and regional DERs are also included in the scope.

Cost

Our assessment is that cost per organization for this NCF is high overall, although costs could vary considerably depending on the degree to which organizations are also responsible for distribution operations and integration of DER systems. Products and services that are used in bulk power generation facilities (e.g., enterprise business IT systems and integrated IT and ICSs) and have vulnerabilities specifically related to quantum computing (not cybersecurity more generally) are likely to receive necessary updates through vendor-provided software or firmware updates or in-cycle hardware replacement. Communication interfaces between bulk power generation facilities, marketplaces, and distribution operations will need to incorporate the new PQC standards in authentication, however, and many organizations that operate electricity generation facilities are also integrated with these functions (Office of Electricity Delivery and Energy Reliability, 2015).

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Furthermore, the heterogeneity of DER systems and the operational complexity of incorporating them into power grids will make it challenging to find easily standardized solutions for DER (Cleveland and Lee, 2013). Integrating DER into electricity distribution requires communication between multiple kinds of communication and distribution technologies and real-time monitoring and control, which are critical to operations for NCF 10, Distribute Electricity (Kuzlu, Pipattanasomporn, and Rahman, 2014). Incorporating PQC (and potentially stronger keys in ICSs in which symmetric keys and hashing are used for security) could introduce additional latency in communications and additional complexity to communication and management systems, and this could lead to significant cost for each affected organization as it addresses how PQC migration uniquely affects its operations (in the case of DERs, see, for example Baker et al., 2018).

Other Factors

Our assessment is that other factors for this NCF are neutral on balance, with exacerbating and mitigating factors identified. Like in NCF 10, Distribute Electricity, the heterogeneity of distribution and power generation systems and regulatory authority across the United States could present a further challenge to interoperability with the diverse ecosystem of power generation facilities, especially DER systems, as the industry migrates to PQC. Many DER systems are customer owned, operate with little external organizational control, use many communication protocols and standards, and might place little emphasis on cybersecurity (Cleveland and Lee, 2013). Although there is evidence of a push toward the use of common standard–based approaches across the industry (see Office of Electricity, undated), these factors could nevertheless make it challenging to coordinate a broader migration to PQC in the industry. This is assessed as a significant exacerbating factor.

The industry is already facing substantial costs as it makes widespread updates to software and hardware to enable greater automation and reliability in electricity distribution (Marston, 2018). This ongoing modernization of the electric grid presents an opportunity to incorporate quantum-resistant solutions in distribution and generation infrastructure as part of ongoing modernization, rather than retrofitting systems later specifically for quantum computing risk mitigation. This is assessed as a mitigating factor.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. Industries often opt to use less vulnerable cryptographic security mechanisms (e.g., preshared symmetric keys or hashing algorithms) in some operational technologies because they require fewer computational resources (Stouffer et al., 2015). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

Priority for Assistance

We rated the NCF as a high priority for assistance. Many organizations in the NCF are affected, and a significant portion of affected organizations could face high costs because of the operational complexity of integration power generation and distribution systems. Although ongoing modernization efforts and layered security in ICSs could provide mitigating factors, the diversity of stakeholders, practices, and interconnected systems in the industry could further complicate a migration to PQC.
References

Works That Informed the Analysis


Cleveland, Frances, and Annabelle Lee, Cyber Security for DER Systems, version 1.0, Electric Power Research Institute, July 2013.


Related Reading


National Critical Function 46, Manufacture Equipment

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>Mitigating and exacerbating factors are present. The NCF could be a likely target for potential threat actors. Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings, on average, lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

- Within a few years of the release of the PQC standard, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets.
- Organizational network access and systems that secure ICSs must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Fabricate and assemble components to produce tangible property” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF could experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit. It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to PQC in communications is delayed. The issues associated with catch-and-exploit vulnerabilities and IP in equipment manufacturing are handled in more depth in our discussion of the assessment for NCF 54, Research and Development.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these
products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.\footnote{This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business information technology systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).}

**Urgency**
Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but these systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**
Our assessment is that other factors for this NCF are neutral, with mitigating and exacerbating factors present. The NCF is a frequent target of cyberattacks (Lexova, 2021), broader industry cybersecurity experience is still developing (Davis, 2017), and U.S. government officials have publicly stated that the theft of U.S. IP by foreign adversaries is a growing concern (Laufman, Casino, and Kasdan, 2020). The reasonable likelihood that a well-resourced attacker with a motivation to steal IP might target this NCF is assessed as an exacerbating factor, although the moderate confidentiality lifetime of most trade secrets limits the impact.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.
Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings, on average, in assessed factors.

References
Works That Informed the Analysis
National Critical Function 47, Produce and Provide Agricultural Products and Services

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>• Within a few years of the release of the PQC standard, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets. • Organizational network access and systems that secure ICSs must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Grow and harvest plant and animal commodities (including crops, livestock, dairy, aquaculture, and timber) and produce inputs required to support agricultural production (such as fertilizers, pesticides, animal food, crop seeds, and veterinary services)” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF might experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit. It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to the use of PQC in communications is delayed. The issues associated with catch-and-exploit vulnerabilities and trade secrets are handled in more depth in our discussion of the assessment for NCF 54, Research and Development.

As agriculture moves toward greater automation and connectivity in operations, networked information technology (IT) and ICSs are becoming more prevalent in operations (DHS, 2018; Yang et al., 2020). The NCF will experience quantum computing vulnerabilities related to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services).

Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., pro-
grammable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.\footnote{This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).}

**Urgency**

Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are mitigating. Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

**Priority for Assistance**

We rated the NCF as a low priority for assistance because of its low ratings, on average, in all assessed factors.
References

Works That Informed the Analysis

DHS, Threats to Precision Agriculture, October 3, 2018.


National Critical Function 48, Produce and Provide Human and Animal Food Products and Services

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in most categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)

• Within a few years of the release of the PQC standard, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets.

• Organizational network access and systems that secure ICSs must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Produce food products from raw agricultural commodities and provide to final consumers (including processing, packaging and production, product storage as well as retail and food service)” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF might experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit. It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to the use of PQC in communications is delayed. The issues associated with catch-and-exploit vulnerabilities and trade secrets are handled in more depth in our discussion of the assessment for NCF 54, Research and Development.

Food processing is dependent on networked business information technology (IT) systems and connected ICSs (Hoffman, 2017; Streng, 2019). The NCF will experience quantum computing vulnerabilities related to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business IT products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of
these products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.¹

Urgency
Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings, on average, in assessed factors.

¹ This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash–based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
References

Works That Informed the Analysis
### Summary

<table>
<thead>
<tr>
<th>Category: Supply</th>
<th>Urgency</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings, on average, lead to a rating of low priority for assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td></td>
<td>- Within a few years of the release of the PQC standard, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Organizational network access and systems that secure ICSs must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
</tr>
</tbody>
</table>

**CISA definition:** "Manufacture basic chemicals from raw organic and inorganic materials and manufacture intermediate and final products from basic chemicals" (CISA, 2020b, p. 6).

### Synopsis of Issues

The NCF might experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit. It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to the use of PQC in communications is delayed. The issues associated with catch-and-exploit vulnerabilities and IP in chemical production are handled in more depth in our discussion of the assessment for NCF 54, Research and Development.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these
products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.\(^1\)

**Urgency**

Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but these systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

**Cost**

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

**Other Factors**

Our assessment is that other factors for this NCF are mitigating. Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

**Priority for Assistance**

We rated the NCF as a low priority for assistance because of its low ratings, on average, in assessed factors.

---

\(^1\) This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business information technology systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
References

Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.


National Critical Function 50, Provide Metals and Materials
Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>Mitigating and exacerbating factors are present. The NCF might be a likely target for potential threat actors. Additional security practices in industrial control system (ICS) networks will often mitigate vulnerability in connected cyber-physical systems.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings, on average, lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>
| Primary concern(s) | • Within a few years, the NCF will need to adopt PQC in communications to protect intellectual property (IP) and trade secrets.  
• Organizational network access and systems that secure ICSs must migrate to PQC before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap. |

CISA definition: “Manufacture iron, steel, and ferro-alloy products; alumina and aluminum products; non-ferrous metals; and other materials as primary components for other industries” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF might experience limited vulnerabilities from catch and exploit of sensitive IP and trade secrets in transit. It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) will be much more common. The cases in which such data have a long confidentiality lifetime and are regularly transmitted using vulnerable communication protocols are likely to be rare enough that they would not lead to significant degradation of the function if captured and exploited, although this vulnerability could become more important if the migration to the use of PQC in communications is delayed. The issues associated with catch-and-exploit vulnerabilities and IP in metal and material manufacturing are handled in more depth in our discussion of the assessment for NCF 54, Research and Development.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, distribution management systems, and other operational technology). Each of these
products and services used by the NCF will need to adopt PQC in the public-key encryption used for authentication prior to the arrival of a CRQC.\textsuperscript{1}

### Urgency

Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Cyber-physical systems and network account access will need to be updated over time through software updates, security patches, and hardware replacements, but these systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

### Scope

Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

### Cost

Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

### Other Factors

Our assessment is that other factors for this NCF are neutral, with mitigating and exacerbating factors present. The NCF is a frequent target of cyberattacks (Lexova, 2021; Sawyer, 2021), and U.S. government officials have publicly stated that the theft of U.S. IP by foreign adversaries is a growing concern (Laufman, Casino, and Kasdan, 2020). The reasonable likelihood that a well-resourced attacker with a motivation to steal IP would target this NCF is assessed as an exacerbating factor, although the moderate confidentiality lifetime of most trade secrets limits the impact.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

\textsuperscript{1} This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business information technology systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Priority for Assistance
We rated the NCF as a low priority for assistance because of low ratings, on average, in assessed factors.

References
Works That Informed the Analysis
———, “National Critical Functions: Status Update to the Critical Infrastructure Community,” July 2020b.
National Critical Function 51, Provide Housing

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Summary</th>
<th>Medium</th>
<th>Post-quantum cryptography (PQC) for key exchange must be implemented after the release of the new standard. Other updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>We identified no other mitigating or exacerbating factors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in most categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s) | Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: “Construct and/or provide safe and secure permanent or temporary shelter for people (includes physical construction and emergency sheltering)” (CISA, 2020b, p. 6).

Synopsis of Issues

The NCF might experience limited vulnerabilities from catch and exploit of sensitive intellectual property (IP) and trade secrets in transit. Organizations in the NCF might regularly transmit sensitive IP and trade secrets related to construction, including blueprints, schematics, construction methods or processes, and other proprietary business information (Reichard, 2018). Construction companies might also transmit designs used for off-site manufacturing, and this could involve the transmission of business-critical information with vulnerable cryptography (Aon, undated). It is expected that, in most cases, such data are at rest on an organization’s network, not in transit, and are therefore not able to be captured. Furthermore, very few trade secrets are expected to have a long confidentiality lifetime (i.e., more than ten years), although trade secrets with a moderate confidentiality lifetime (i.e., one to ten years) might be more common. This vulnerability will become more important over time if the migration to the use of PQC for key exchange in communications is delayed.

This NCF will experience authentication vulnerabilities in products and services provided by other NCFs, and it will depend on those NCFs to address vulnerabilities. This NCF will be especially dependent on authentication vulnerabilities being addressed in products and services from NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services. These vulnerabilities arise from the ubiquitous use of public-key cryptography to identify and authenticate users and equipment across the Internet. These products and services must migrate to use PQC for remote authentication before a cryptographically relevant quantum computer arrives.1

---

1 This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities lie in their reliance on Internet-accessible resources and networked business information technology (IT) systems. We assessed that this group included NCFs 20, 21, 26, 27, 28, 31, 36, and 51. The assessments for these NCFs are similar in many respects. These NCFs do not handle data with a long secrecy lifetime, so their primary concern will be managing configuration changes, software updates, and in-cycle hardware replacements needed to migrate to PQC in Internet-dependent IT products and services provided by other NCFs.
Urgency
Our assessment is that urgency of action for this NCF is medium. Most IP and trade secrets are likely to have a moderate or short confidentiality lifetime, and the NCF will need to adopt PQC for key exchange in communications within a few years of the release of the PQC standard. Networked business IT systems will need to be updated over time through software updates, security patches, and hardware replacements, but these systems need complete updates only before a cryptographically relevant quantum computer arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low because most affected products and services are provided by other NCFs and those NCFs will be responsible for providing updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are neutral. We identified no additional mitigating or exacerbating factors for this NCF.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in most assessed factors.

References
Works That Informed the Analysis
Aon, “Cyber Vulnerability in the Construction Sector,” webpage, undated.
National Critical Function 52, Provide Information Technology Products and Services

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Urgency</th>
<th>High</th>
<th>The national critical function (NCF) will need to rapidly provide the products and services other NCFs need to address their catch-and-exploit vulnerabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>High</td>
<td>Nearly every organization producing software or hardware that facilitates interactions over networks will be required to make an update to address vulnerabilities.</td>
</tr>
<tr>
<td>Cost</td>
<td>High</td>
<td>Actions to address vulnerabilities are likely to involve extensive development, testing, and integration of both hardware and software in most cases.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>Both mitigating and exacerbating factors are present. The NCF is a critical dependency for others, and incentives might not be aligned to move as rapidly as needed. Fortunately, evidence suggests that many organizations are already proactively developing solutions.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>High</td>
<td>The NCF has a high urgency, scope, and cost per organization that are not mitigated. Despite the efforts of early movers, many organizations are likely to benefit from assistance.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td>The NCF is a critical dependency for most other NCFs to mitigate vulnerabilities from quantum computing. There is a risk of enduring, widespread vulnerabilities in other NCFs if information technology (IT) products and services are not readily available to facilitate the migration to post-quantum cryptography (PQC). Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.</td>
<td></td>
</tr>
</tbody>
</table>

CISA definition: “Design, develop, and distribute hardware and software products and services (including security and support services) necessary to maintain or reconstitute networks and associated services” (CISA, 2020b, p. 6).

Synopsis of Issues
The greatest impacts of catch-and-exploit vulnerabilities in this NCF would fall on customers rather than the providers. A previous DHS assessment of this NCF noted that “the distribution or production of an untrustworthy product or service is of greater relative concern than risks associated with the ability of the Sector to produce or distribute hardware, software, and services” (DHS, 2009, p. 27). The most important catch-and-exploit vulnerability for this NCF therefore centers on the NCF’s role in producing trustworthy products to consumers. The failure to produce products and services that can secure consumers’ data with a long confidentiality lifetime against a catch-and-exploit campaign would constitute the delivery of untrustworthy products. The previous assessment further stated that

the tangible consequences from this could include the loss of intellectual property; identification of key personnel on projects or products; loss of brand image; possible degradation of the overall system or function being provided by multiple entities; and significant economic impacts . . . . (DHS, 2009, p. 27)

Provision of products that led to these consequences would constitute a significant degradation or disruption of this NCF. Providing organizations in the NCF might also experience catch-and-exploit vulnerabilities that affect the confidentiality of their intellectual property (IP). It is assumed, however, that data associated with such IP are rarely in transit (and thus not subject to capture), and those data are likely to have a short confidentiality lifetime, given the fast pace of technological change in this NCF. Where either of these two
assumptions holds true, the potential impact of catch-and-exploit campaigns to steal IP from IT product and service providers would be low.

The authentication vulnerabilities affecting this NCF are related primarily to the instances in which functions of IT products and services are facilitated by connections to other networks, and this portion of the assessment is therefore very similar to that for NCF 3, Provide Internet Based Content, Information, and Communication Services. Nearly every instance in which IT products currently facilitate a presumed secure, remote interaction with a network will present an authentication vulnerability when a cryptographically relevant quantum computer (CRQC) exists. The primary authentication vulnerabilities affecting this NCF stem from the ubiquitous use of digital signatures and public-key infrastructures (PKIs) to identify entities on a network. Although some aspects of these tools are more appropriately described in NCF 35, Provide Identity Management and Associated Trust Support Services, the use of digital signatures and digital certificates are of particular relevance to the authentication vulnerabilities in this NCF. Digital signatures and certificates use public-key cryptography to identify entities on the network and confirm authenticity in online interactions. Quantum computing will enable an attacker to derive the private cryptographic keys associated with these tools, allowing the attacker to falsely identify itself as nearly any user or organization that uses these tools to secure access to a network. This assessment will not attempt to enumerate the many categories of IT products and services that facilitate remote interactions using digital signatures and PKI in some way; suffice it to say that it might be easier to enumerate those that do not. Like in NCF 3, the most troubling of the potential authentication vulnerabilities will be those that have the capacity to have systemic security effects across the ecosystem of IT products and services, such as if an attacker exploited a vulnerability to receive root access to databases of other cryptography keys held in the cloud (e.g., database read–write keys held in Microsoft’s Cosmos DB database; see Menn, 2021).

**Urgency**

Our assessment is that urgency of action for this NCF is high. Every instance (or very nearly so) of a catch-and-exploit vulnerability involves the use of IT products and services in some way. As a result, it is imperative that IT products and services be available as soon as practical that can facilitate the use of PQC for key exchange in communications of data with a long confidentiality lifetime.

Providers of products and services that use digital signatures and PKI to authenticate users and organizations in remote interactions will need to move to PQC only before a CRQC is available to attackers. The migration to new standards across the Internet is historically long and slow, however, and there will likely still be many unaddressed authentication vulnerabilities in place when that time comes (Vermeer and Peet, 2020). If the move to PQC is not prioritized by the many product and service providers across this NCF, it might not be possible to deprecate old, vulnerable standards when a CRQC arrives. Authentication issues therefore also contribute to an assessment of a high urgency for this NCF, and organizations should immediately begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

**Scope**

Our assessment is that scope for this NCF is high. Nearly every organization producing software or hardware that facilitates interactions over networks will be required to make an update to address vulnerabilities. This constitutes a large number of organizations. Although the scale of the effort could vary significantly depending on what role each organization plays in delivering this NCF, each one will need to update its product in some way to enable the use of PQC in secure online interactions.
Cost
Our assessment is that cost per organization for this NCF is high overall, although there is likely to be significant variation. The migration to PQC in IT products and services is likely to involve substantial development and testing in both hardware and software products. The NCF produces products and services that require broad compatibility with many other networked software applications and hardware components. As the requirements of PQC for different hardware and software products become known, those products will need to be developed then tested by this NCF to ensure forward and backward compatibility with other products and services. Many of the relevant products and services are highly complex (DHS, 2009), and implementing hybrid PQC schema could further add to that complexity and create challenges. In one set of experiments testing the use of a hybrid PQC scheme in secure web connections using transport-layer security (TLS), for example, it was discovered that “non-compliant network middleware” (software and hardware designed to handle a variety of secondary services and capabilities for an operating systems) was causing connection failures (Chromium Projects, undated; Cimpanu, 2021). It will likely be costly to perform the development and testing necessary to quickly produce products that do not cause complex failures or performance issues that would broadly disincentivize or disable the adoption of PQC.

Other Factors
Our assessment is that other factors for this NCF are neutral, with a balance between exacerbating and mitigating factors. We identified the following exacerbating factors:

- Nearly every other NCF depends on this NCF in some way to quickly produce the products and services needed to execute the migration to PQC. If this NCF does not make IT products and services that can accommodate PQC available as quickly as is needed, vulnerability will remain in place in other NCFs. This would increase the risk from catch and exploit across critical infrastructure and could make it challenging to ensure complete adoption of PQC in authentication prior to the arrival of a CRQC.

- Organizations in this NCF will often have little vulnerability in their own operations that would require them to adopt PQC quickly themselves. In some instances, their customers might also not know or understand the urgency of migration to PQC to protect sensitive data. Finally, this NCF often experiences intense pressure to deliver low-cost products quickly (DHS, 2009). If few organizations see competitive advantage in creating products that can accommodate PQC, the cost of the development and testing needed to create PQC-compatible products and services might not be viewed as justified, and the migration could be delayed.

Fortunately, a significant mitigating factor is present. Evidence suggests that many large organizations in the NCF understand the importance of these issues and have been proactively working to develop products and services with PQC compatibility and cryptographic agility in mind. Efforts are being made to develop and test software that can support PQC in secure web connections and cloud services, and the Trusted Computing Group (TCG) has issued guidance for secure update of software and firmware in embedded systems, with cryptographic agility needed for the PQC transition in mind (TCG, 2020). Some organizations, such 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). These example activities from industry groups and significant organizations in this NCF suggest that broader effort toward PQC transition in the NCF might be underway.
Priority for Assistance
We rated the NCF as a high priority for assistance. The urgency, scope, and cost per organization are all rated as high. This NCF is critically important to the overall transition to PQC, and it is likely that a very large number of organizations will need to move quickly to produce updated products and services, often incurring high costs for development because of the complexity of products, supply chains, and interoperability requirements. Although some major organizations in this NCF are well resourced and proactively addressing this issue, there are likely to be many other organizations that will benefit from assistance. That assistance could include coordination of development efforts and priorities across the NCF, financial incentives to offset costs and motivate development, and dissemination of technical guidance and standards.

References
Works That Informed the Analysis
Chromium Projects, “CECPQ2,” webpage, undated.
DHS, Information Technology Sector Baseline Risk Assessment, August 2009.

Related Reading
National Critical Function 53, Provide Materiel and Operational Support to Defense

Category: Supply

Summary

<table>
<thead>
<tr>
<th>Factor</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>High</td>
<td>This national critical function (NCF) handles a large amount of data in transit with a long confidentiality lifetime.</td>
</tr>
<tr>
<td>Scope</td>
<td>High</td>
<td>This NCF has many dispersed organizations that might need to individually address updates.</td>
</tr>
<tr>
<td>Cost</td>
<td>High</td>
<td>This NCF uses highly specialized noncommercial hardware and software and faces unique security requirements.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Neutral</td>
<td>An exacerbating factor is that threat actors with the resources for a catch-and-exploit campaign might have motivation to target this NCF. Mitigating factors are that affected NCF organizations have extensive cybersecurity experience and resources, and they have experience complying with National Security Agency/ Central Security Service (NSA/CSS)–ordered encryption requirements. The U.S. government can directly promote adoption to post-quantum cryptography (PQC) via contractual requirements on its vendors.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>High</td>
<td>This NCF handles a large amount of data in transit with long confidentiality lifetimes, and mitigation actions will have high cost and (potentially) high scope.</td>
</tr>
<tr>
<td>Primary concern(s)</td>
<td></td>
<td>This NCF is a likely target for a threat actor with the resources required to conduct a catch-and-exploit campaign, and the unauthorized disclosure of sensitive data in transit could cause exceptionally grave damage to national security.</td>
</tr>
</tbody>
</table>

CISA definition: “Develop, produce, and sustain defense systems and components and provide support to defense operations” (CISA, 2020b, p. 6).

Synopsis of Issues

This NCF faces very serious catch-and-exploit vulnerabilities due to its use of vulnerable public-key cryptography algorithms in networked communications. The U.S. defense industrial base transmits sensitive defense-related information between its organizations, the U.S. Department of Defense, and other agencies that deal with national security. In some cases, this includes classified information. Although the unauthorized interception of unclassified information transmitted by the defense industrial base poses risks to the functioning of this NCF, the most-serious risks come from the interception of classified information. As laid out in Executive Order (EO) 13526, the unauthorized disclosure of classified information could reasonably be expected to cause damage to national security (or serious or exceptionally grave damage, depending on the level of classification). EO 13526 specifies that, by default, classified information remains classified for ten years after its creation, but original classification authorities are authorized to extend this classification period to 25 years (or longer, under certain circumstances laid out in the EO). The confidentiality lifetime of such information is long enough that mitigation actions need to be taken long before a cryptographically relevant quantum computer is developed.

NSA/CSS has publicly announced plans for transitioning to PQC algorithms for the transmission of classified information. In the interim, the agency has publicly authorized the use of public-key cryptography algorithms, such as Rivest–Shamir–Adleman (RSA) that are vulnerable to a quantum computer (NSA/CSS, 2015). After National Institute of Standards and Technology completes its selection process for PQC algorithms, NSA/CSS will issue updated guidance for operators of national security systems (NSSs) through Committee on NSSs Policy 15 (Committee on NSSs, 2016; NSA/CSS, undated). The sooner that NSS opera-
tors transition to PQC after this guidance is released, the less classified and other national security information will be at risk of intercept.

The NCF also faces serious authentication vulnerabilities. A threat actor that gains access to databases containing (potentially classified) defense-related information could exfiltrate, encrypt, erase, or modify critical technical or intelligence information, thereby degrading the performance of the NCF. There could also be a risk of cyber-physical systems access that could seriously degrade the performance of defense systems. Although these are just-in-time risks that can be addressed any time before the advent of a cryptographically relevant quantum computer, it is critical to the functioning of the NCF that every mode of remote authentication for defense-related systems be migrated to PQC before then.

**Urgency**
Our assessment is that urgency of action for this NCF is high. Defense-related information (particularly classified information) has both an exceptionally long confidentiality lifetime and exceptionally grave consequences of unauthorized disclosure. The sooner the encryption for data in transit migrates to PQC algorithms, the less defense-related information will be vulnerable to a catch-and-exploit campaign.

**Scope**
Our assessment is that scope for this NCF is high. Thousands of organizations provide support to the Department of Defense in some way (FactSet, 2021). Although the actions each organization will need to take might vary considerably, the number that will need to take meaningful action of some kind to protect sensitive data is likely well above the threshold (at least 100 organizations) for a rating of high scope.

**Cost**
Our assessment is that cost per organization for this NCF is high overall, although there is likely to be significant diversity in the level of effort required of organizations in this NCF. Some organizations might need to make changes as simple as altering security configurations, but many will need to perform out-of-cycle replacements of networking hardware or extensive development of software and hardware that can conform to the new PQC standard. Some NSSs and components might have specialized security requirements that require custom solutions. These systems might require off-cycle component replacements.

**Other Factors**
Our assessment is that there are both mitigating and exacerbating other factors for this NCF. Threat actors possessing the significant resources required for a catch-and-exploit campaign might well have a strong motivation to target defense-related communications, and this presents a strong exacerbating factor.

We also identified several mitigating factors. Most organizations that provide support related to NSSs will likely already have the cybersecurity expertise and resources needed to meet current requirements, including the strict encryption requirements issued by NSA/CSS, which will also manage the transition to PQC algorithms. Although a large number of organizations operate NSSs, the U.S. government has established procedures for inspecting and certifying NSSs. Finally, the U.S. federal government is the ultimate end purchaser of all U.S. defense materiel, so the government can directly promote all of its vendors’ implementation of PQC by issuing contractual requirements that any defense systems that it purchases must use PQC (if applicable).

**Priority for Assistance**
We rated the NCF as a high priority for assistance because of its high ratings in all assessed factors.
References

Works That Informed the Analysis
FactSet, financial data and analytics, 2021.
NSA/CSS, “Quantum Key Distribution (QKD) and Quantum Cryptography (QC),” webpage, undated.
National Critical Function 54, Research and Development
Category: Supply

Summary

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Urgency</strong></td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Low</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Low</td>
</tr>
<tr>
<td><strong>Other factors</strong></td>
<td>Neutral</td>
</tr>
<tr>
<td><strong>Priority for assistance</strong></td>
<td>Low</td>
</tr>
</tbody>
</table>

Most organizations involved with this national critical function (NCF) handle data with a confidentiality lifetime that is less than ten years, although some exceptions have longer confidentiality lifetimes.

Only a few organizations would need to take active mitigation measures.

Mitigation is likely to take place through software updates and in-cycle hardware replacement for most organizations and the purchase of a limited number of commercial off-the-shelf systems for the remaining organizations.

A relatively small number of well-known industry targets could make targeted exploitation worthwhile, but these organizations will have significant experience and resources for cybersecurity.

Only a small number of organizations involved with this NCF will need to take proactive action (at low cost) to address catch-and-exploit vulnerabilities.

Some commercial organizations conduct research and development (R&D) that requires valuable intellectual property (IP) with long confidentiality lifetimes. These organizations might need to adopt post-quantum cryptography (PQC) faster than other companies in order to protect their trade secrets. All organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.

CISA definition: "Conduct basic research, innovate, test, and introduce new products and services or improve existing products and services" (CISA, 2020b, p. 7).

Synopsis of Issues

Some NCF subfunctions could experience significant catch-and-exploit vulnerabilities. Basic research and product testing generally do not require transmitting information with long confidentiality lifetimes: Basic (as opposed to applied) research contributes to general scientific knowledge and so is usually made public upon completion, while product testing is performed on products that are fairly close to market. However, the process of introducing new products and services (i.e., industrial R&D) can require the internal exchange of trade secrets (e.g., between different laboratories within the same corporation) that can sometimes have a long confidentiality lifetime; for example, one study estimated that, in the pharmaceutical industry, the process of developing a new drug has an average length of 10.5 years (Austin and Hayford, 2021). Catch-and-exploit opportunities could degrade the performance of these industries with long R&D lifetimes, but most industry R&D life cycles are not as long as the pharmaceutical industry's.1

The major authentication vulnerabilities to this NCF stem from the potential for compromised institutional network access that could lead to the theft of industry trade secrets or disruptions to operations. Although there have been a few large-scale thefts of academic data from universities (Office of Science and Technology Policy, 2020), the U.S. government has identified the theft of U.S. trade secrets as a major concern that goes far beyond basic research (Defense Security Service, 2013). Although damaging or falsifying R&D data as a form of industrial sabotage is possible, industrial espionage through the theft of technical data or trade secrets by itself would be enough to seriously degrade the performance of the NCF. Although it is

---

1 Major defense contractors that produce sophisticated military platforms are another class of organization with R&D life cycles that can span decades. We consider these functions separately as part of NCF 53, Provide Materiel and Operational Support to Defense.
expected that commercial organizations keep industrial R&D confined to internal networks, the increasing prevalence of remote work and access through virtual private networks (VPNs) reliant on public-key cryptography would lead to vulnerabilities in these networks that could put these data at risk.

Urgency
Our assessment is that urgency of action for this NCF is medium overall. For basic research institutions, such as universities, it is low because little of their data is likely to have a long confidentiality lifetime. Many industrial organizations carry out internal R&D that generates valuable trade secrets with a moderate confidentiality lifetime, although a few organizations might have R&D life cycles longer than ten years. For these few organizations, the urgency is high if these data are ever in transit. There are also significant authentication vulnerabilities, but these pose just-in-time risks that can be mitigated through routine software updates, security patches, and in-cycle hardware replacement. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low. A relatively small proportion of commercial organizations conduct R&D with a long confidentiality lifetime, and, in most cases, any sensitive data will be stored at rest in internal databases. Therefore, few organizations need to take active, swift risk-mitigation efforts.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement. The few organizations that might need to address more-urgent catch-and-exploit vulnerabilities will likely need to buy only a limited amount of commercial off-the-shelf hardware or software that conforms to PQC standards to secure any sensitive IP that must be transmitted.

Other Factors
Our assessment is that other factors for this NCF are neutral on balance, with mitigating and exacerbating factors present. A relatively small number of organizations have very long R&D cycles that generate critical IP, and most of these companies are large and well resourced. The fact that there are relatively few potential targets might make it feasible for a threat actor to target them individually, which is an exacerbating factor. However, most of these organizations have significant experience and resources for cybersecurity, including existing special systems and procedures for handling sensitive data, which will ease the transition to PQC and is a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of the limited number of organizations that will need to take proactive actions against catch-and-exploit vulnerabilities and the low cost of these mitigations.

References
Works That Informed the Analysis

Related Reading
National Critical Function 55, Supply Water
Category: Supply

Summary

<table>
<thead>
<tr>
<th>Category</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgency</td>
<td>Low</td>
<td>Updates can happen gradually, provided that they are complete when a capable quantum computer arrives.</td>
</tr>
<tr>
<td>Scope</td>
<td>Low</td>
<td>Issues will be addressed largely by other national critical functions (NCFs). Situations requiring active, swift risk mitigation are likely to be rare.</td>
</tr>
<tr>
<td>Cost</td>
<td>Low</td>
<td>Mitigation is likely to take place through software updates and in-cycle hardware replacement.</td>
</tr>
<tr>
<td>Other factors</td>
<td>Mitigating</td>
<td>The water and wastewater sector is well-supported by various groups, and additional security practices in industrial control system (ICS) networks will often mitigate vulnerability.</td>
</tr>
<tr>
<td>Priority for assistance</td>
<td>Low</td>
<td>Low ratings in all categories lead to a rating of low priority for assistance.</td>
</tr>
</tbody>
</table>

Primary concern(s)
Organizational network access and systems that secure ICSs must migrate to post-quantum cryptography (PQC) before a cryptographically relevant quantum computer (CRQC) is available. Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap.


Synopsis of Issues
The NCF is unlikely to experience significant vulnerabilities from catch and exploit. We identified no examples of data with a long confidentiality lifetime that might be regularly transmitted.

Other quantum computing vulnerabilities affecting this NCF relate to public-key cryptography–based authentication in products or services provided by other NCFs (specifically, NCF 3, Provide Internet Based Content, Information, and Communication Services, and NCF 52, Provide Information Technology Products and Services). Authentication vulnerabilities will be present in networked business information technology (IT) products and services used to support operations (e.g., cloud-based services and applications for communication, remote network access, and enterprise resource management) and in integrated cyber-physical systems and components (e.g., programmable logic controllers, ICS or supervisory control and data acquisition [SCADA] systems, process control systems, distribution management systems, and other operational technology). Wherever public-key encryption is used for authentication, each of these products and services used by the NCF will need to adopt PQC prior to the arrival of a CRQC.¹

¹ Water and wastewater are typically treated as a single sector, and they share most of the same organizations and vulnerabilities. As a result, the assessments for NCF 25, Manage Wastewater, and NCF 55, Supply Water, are largely identical. This NCF is part of a group of NCFs whose primary quantum computing vulnerabilities arise from the use of networked business IT systems and ICSs. We assessed that this group included NCFs 10, 12, 14, 16, 17, 18, 24, 25, 41, 43, 44, 45, 46, 47, 48, 49, 50, and 55. The assessments for these NCFs are similar in many respects. ICSs are increasingly standardized and connected to enterprise networks for remote monitoring and control. As part of the security policy for those networks, public-key infrastructures and other cryptographic security mechanisms are often used to identify users and devices and secure these networks (Industrial Control Systems Cyber Emergency Response Team [ICS-CERT], 2016; Stouffer et al., 2015). Public-key cryptography–based security mechanisms (and, in some cases, weak symmetric-key or hash-based security) will create quantum computing vulnerabilities in these networked systems. There are numerous historical examples of conventional cyberattacks targeting systems such as these, leading to disruptions to operations (Hemsley and Fisher, 2018).
Urgency
Our assessment is that urgency of action for this NCF is low. Cyber-physical systems and IT network access will need to be updated over time through software updates, security patches, and hardware replacements, but systems need complete updates only before a CRQC arrives. Organizations should nevertheless begin early preparations for the PQC migration by following the steps outlined in the DHS roadmap.

Scope
Our assessment is that scope for this NCF is low. Although more than 150,000 public water systems supply water in the United States (DHS and EPA, 2015), it is unlikely that these organizations will need to actively address the vulnerabilities. Most affected products and services are provided by other NCFs, and those NCFs will address the required updates. As a result, appropriate actions from organizations in this NCF are likely to happen over time with limited engagement, and situations requiring active, swift risk mitigation are likely to be rare.

Cost
Our assessment is that cost per organization for this NCF is low. Organizations should begin to follow the preparation steps outlined in the DHS roadmap. When the PQC standard is released, organizations will likely be able to migrate to PQC over time as part of conventional cybersecurity efforts, such as configuration changes, software updates, security patches, and in-cycle hardware replacement.

Other Factors
Our assessment is that other factors for this NCF are mitigating. The water and wastewater sector is well supported by many public and private organizations and associations, including the Water and Wastewater Systems Sector Coordinating Council, Water and Wastewater Systems Government Coordinating Council, Water Information Sharing and Analysis Center, and various other affiliated organizations (see DHS and EPA, 2015, Appendix 3). These groups are coordinating to develop cybersecurity resources for the sector, and state and federal regulations are increasingly requiring water-system operators to address and prioritize cybersecurity (Germano, 2019). These are seen as a mitigating factor.

Although networked ICSs present a vulnerability, deployed ICS technology is often resource-constrained. 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). Networked ICSs often also rely on additional, redundant 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). This presents a mitigating factor.

Priority for Assistance
We rated the NCF as a low priority for assistance because of its low ratings in all assessed factors.

References
Works That Informed the Analysis


**Related Reading**