Comments in response to NIST Cyber Security Framework Draft 1.1 and NIST Roadmap for Improving Critical Infrastructure Cybersecurity Draft 1.1

Submitted by:

Tyson Macaulay, Advisory Board Member, InfoSec Global
Tyson.macaulay@infosecglobal.com
+16132929132

Reviewers:

Tomislav Nad, Chief Security Architect & Cryptographer, InfoSec Global
Bill Munson, Director, Research and Policy Analysis, Quantum-Safe Canada, University of Waterloo
Vladimir Soukharev, Cryptographer, InfoSec Global
Dr. Michele Mosca, CEO, evolutionQ Inc., and Co-Founder, Institute for Quantum Computing, University of Waterloo

Table of Contents

Summary:

At this time Cyber Security Framework and the Roadmap are silent on the effects on cryptography presented by emerging quantum computing technologies, and the need to develop **Cryptographic agility** and engage in **Quantum Risk Management.**

Cryptographic agility refers to the ability to actively monitor and manage the encryption and related verification technologies deployed across an organization.

Quantum risk derived from the emergence of quantum computing technologies, which will generate major vulnerabilities in the most widely deployed, conventional cryptography in the near future (with significant probability in the next 8 to 10 years but outside chances of as little as 5 years).

Cryptographic Agility is the major remediation and control for managing Quantum Risk, and fosters forward-compatibility for critical and non-critical information system alike.

Planning and preparedness for post-quantum technology is a fundamental element associated with the security and resilience of all critical infrastructure, because of the need to consider the time required for integration and the period for which secrets must be maintained (data remains confidential) beyond the advent of quantum computing.

It is our belief that the Cyber Security Framework or at least the Roadmap should include guidance associated with these issues of **Cryptographic Agility** and **Quantum Risks**.

Introduction

Main question posed by NIST related to Draft 2 of the Cyber Framework:

> *"Do the revisions in Version 1.1 Draft 2 reflect the changes in the current cybersecurity ecosystem (threats, vulnerabilities, risks, practices, technological approaches), including those developments in the Roadmap items?"*

No, neither the Cyber Security Framework, the Roadmap nor the underlying NIST 800-53r4 *Security and Privacy Control for Federal Information Systems* nor NIST 800-161 *Supply Chain Risk Management* mention the need to consider **cryptographic agility**, or **quantum computing risks** and their impact on the most widely used forms of security today.

Cryptography is the foundation of our digital world. It is present is virtually all applications, platforms and communications network in some form for the purposes of both encryption and authentication.

Cryptography underlies everything from consumer solutions for banking to social media to government services. The same cryptographic technology underlies all Enterprise solutions for secure Internet infrastructures to protecting databases full of personal information, trade secrets and national security information in the realm of government and public safety.

Cryptographic AGILITY; stepchild of information security.

Cryptographic agility refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. This includes the ability to deploy, monitor, provision/update and disable/de-commission cryptography features and functions without wholesale shutdown, OS patching or re-installation, or physical replacement of the asset.

A cryptographic agile security design should provide:

- **Manageability**：
  Usage of cryptographic algorithms must be manageable separately from the application.
- **Implementation independence:**
  Application code must be independent from cryptographic implementations.
- **Implementation simplicity:**
  The interface to cryptography must be simple to reduce the risk of usage errors.
- **Dynamic exchangeability and extensibility**：
  Systems must be able to change cryptographic algorithms dynamically. Systems must be able to add new algorithms dynamically.

Cryptography lies buried at the heart of of information-driven world. Unbeknowst to most people, cryptography touches just about every application, platform and network, used by consumers, business and government alike. See Figure 1: Cryptographic agility. As a result, cryptographic agility benefits just about every part of a modern society; while static, ridig cryptographic services pose risks.

For lack of cryptographic agility, weaknesses and vulnerabilities in cryptography are difficult to identify, manage and remediate.

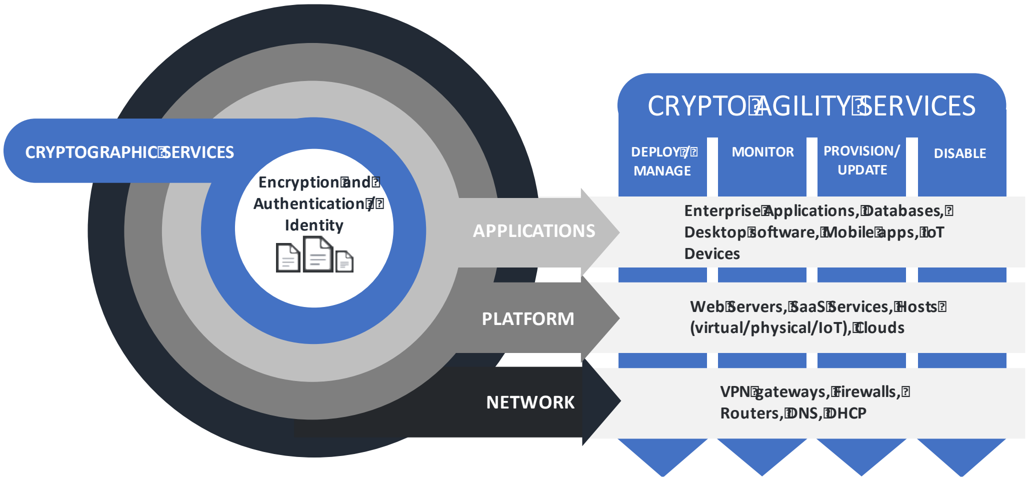
CRYPTOGRAPHIC SERVICES
Encryption and Authentication / Identity
APPLICATIONS
PLATFORM
NETWORK
CRYPTO AGILITY SERVICES
DEPLOY / MANAGE
MONITOR
PROVISION/ UPDATE
DISABLE
Enterprise Applications, Databases, Desktop Software, Mobile apps, IoT Devices
Web Servers, SaaS Services, Hosts (virtual/physical/IoT), Clouds
VPN gateways, Firewalls, Routers, DNS, DHCP

Figure 1: Cryptographic agility

A lack of cryptographic agility is essentially the state of the market in 2018, where any update to address a weakness or flaw is typically a system-by-system, manual process of downtime, OS patching, re-installation and sometimes premature end-of-life.

The price of overlooking cryptographic agility is growing by the day. Consider one example from 2014: the Heartbleed Bug[1]. This is a vulnerability in the OpenSSL cryptographic software library, which allows threat actors to steal information protected by the SSL/TLS encryption. It took more than 800 days to identify it, and cost more than $500 million to fix—and years later, nearly 200,000 websites are still at risk[2].

A most recent and equally serious example from 2017 is a vulnerability in the cryptographic library from 2012[3] producted by Infineon and used by many high assurance applications for

[1] https://en.wikipedia.org/wiki/Heartbleed
[2] https://thehackernews.com/2017/01/heartbleed-openssl-vulnerability.html
[3] https://crocs.fi.muni.cz/public/papers/rsa_ccs17

government and commercial entities globally. The vulnerability is especially problematic as it is located in code that complies with two security certification standards, NIST FIPS 140-2 and CC EAL5+ intended to explicitly AVOID the risk of cryptographic flaws in software and hardware. It may take years to provide a fix (or more likely replace) for all instances of the vulnerability, even if it is possible to identify all affected assets.

Other examples of serious vulnerabilities that become difficult or impossible to manage without formalized agility include the growing number if IoT devices, which tend to be deployed and forgotten – until their security is compromised, often well before their amortization is complete[4]. Improved agilty might also address the consistently, poorly configured security which even some of the best-resourced service providers on the Internet – like banks – cannot seem to get right for lack of the ability to centrally monitor and update cryptographic settings in online services – let along address flaws in cryptographic libraries.[5],[6],[7]

In order to make future instances of such problems easier to address, security systems have to support cryptographic agility, and agility should play a central role in the security design.

[4] https://www.theregister.co.uk/2017/08/31/arms_embedded_tls_library_patched_to_fix_mitm_bug/

[5] http://www.theregister.co.uk/2017/12/13/robot_tls_rsa_flaw/

[6] https://www.keycdn.com/blog/http-security-headers

[7] https://securityheaders.io/

QUANTUM risk; no light just a train.

NIST as an organization is well aware of the quantum "threat" and is a leading light in the develop of post-quantum cryptographic solution and standards; however, this leadership now needs to be incorporated into other forms of industry guidance, such as the Cyber Security Framework and the underlying NIST 800-53r4 and NIST 800-161 – Supply Chain Risk Management.

The factoring of very large numbers and finding discreet algorithms is core to what is known as asymmetric cryptography or public key cryptography. This form of cryptography underpins virtually all modern security, from consumer to military applications and systems. See Table 1.

	Consumer	Business / Enterprise	Public safety / Government
Applications, Platforms and Networks vulnerable to quantum risks	Smartphones/laptops/ tablets/desktop Everything "on-line" • Shopping • Banking • Social networking • Web searches • Personal email • Smart cars • Smart homes	• Telecoms network security • Database security • Data Centre security • Branch office communications • Remote workers • Smart cities • Critical infrastructure • Intellectual property	• National Security communications • State secrets • Army/Navy/Air force command and control • Smart tanks, ships, and planes • Ports and infrastructure • Physical security monitoring • Front-line communications

Table 1: Applications, Platforms and Networks with quantum risks

Effective quantum computers eliminate the strength of current public key crypto-system we rely upon. In general, cryptography can be classified into two subgroups – public-key and symmetric.

For the symmetric side (such ciphers as AES), one needs to only double the size of the key length, to maintain quantum resistance. This is due to the fact, that the only quantum algorithm discovered for symmetric ciphers is Grover's algorithm, which performs searches in square-root time.[8]

[8] https://en.wikipedia.org/wiki/Grover%27s_algorithm

Looking at the public-key cryptography, which usually underlies symmetric key-agreement and digital signatures, can be easily broken by a moderately scaled quantum computer. Thus, public-key side needs a total replacement or upgrade in the post-quantum world. Because key agreement and signatures are so fundmental to most modern information systems – as discussed - they are the ones that require the most attention and need to be replaced with post-quantum algorithms as soon as possible.

Because effective quantum computers are considered to have an even chance of becoming a reality in the next 8 to 10 years[9] (with odds improving all the time), the time to start acting is now.

Why now? In 2018?

Most people initially overlook the question of how long do they need their data to remain secret and secure (*unavailable* without authorization and *unchanged* without permission). In other words, what is the **"shelf life"**[10] of the encryption applied?

Even if data has no specific shelf-life, it has quantum-computing risks. For instance, issues related to intellectual property licensing's (like copyright) and forgery (corruption) can be risks to even public-domain information or broadcast media.

The shelf life of information will vary depending on the nature of the data itself.

Table 2: Shelf life of encrypted information - proposes a simple overview of the types and owners of data, the typical shelf-life they might apply to their data as a matter of privacy, regulation, national security or contracted obligations.

[9] Michele Mosca, University of Waterloo Centre for Quantum Computing, 2017

[10] Michele Mosca, Cybersecurity in an era with quantum computers: will we be ready?, University of Waterloo Insitute for Quantum Computing, 2015.

Table 2: Shelf life of encrypted information

	Consumer data[11]	Business / Enterprise data	Public Safety / National Security data
Minimum Shelf life of data	<5 years	>7 years	>20 years
Examples	• Personal Tax and Financial records • Health records	• Sales and Taxation records • Customer, Partner and Supplier information • Regulatory compliance data • Business strategy and plans • Intellectual property • Media and copyright-protected materials[12]	• National security (classified) information

[11] Much of the risk to consumer data will not be legal or physical in nature, rather it will be the personal loss or embarrassment of having losing control of all personal information, everything from family photos to confidential discussions with friends and family.

[12] Copyright protection lasts for the life of the author + 70 years in the United States and UK, and the life of the author + 50 years in Canada.

Time to retro-fit

The next major consideration in quantum risk management is the *time it will take to re-tool and deploy existing systems with quantum-safe algorithms*[13].

How long to develop, test and stabilize network security such as SSL, TLS, and IPSec VPNs used all around the world for everything from gaming networks to military communications channels?

How long will it take to upgrade, test and stabilize applications security software, including everything from massive databases of transaction or legal information going back decades, all the way to social media apps on smartphones?

Finally, how long will it take to not only deploy the quantum safe upgrades – but also de-commission, uninstall and end support on vulnerable, pre-quantum software and applications? We cannot make post-quantum algorithms backward compatible, as otherwise we would only have classical security, but no quantum resistance.

Table 3 is representation of retro-fit requirements for consumers, business and government.

	Consumer IT	Business/Enterprise/ Government IT	Critical Infrastructure / Industrial Operational Technology (OT)
Time to retrofit	>2 year	> 6 years	10 to 30 years
Examples of things to retrofit	Patch Smartphones/laptops/ tablets/desktop Replace Smartphones/ laptops/ tablets/desktop when vendor support / patching not available or possible. De-commission and end support on vulnerable products and services.	Consumer IT + Patch / upgrade / replace all database and storage infrastructure Patch / upgrade / replace all on-line service-delivery portals and interfaces. Patch / upgrade / replace all in-field equipment and internet-connected Industrial IoT. De-commission and end support on vulnerable products and services.	Consumer and Business/Government IT + Patch / upgrade / replace embedded systems Replace / Amortize infield and factory floor components across centralized and remote monitoring and control systems. De-commission and end support on vulnerable products and services.

Table 3: Time need to retro-fit for quantum risks

[13] Ibid, Michele Mosca.

The quantum risk equation

If the time to integrate quantum safe cryptography, plus the shelf life of sensitive data, exceeds the time to an effective quantum computer, you have “quantum risk”. Specifically, the planned shelf-life may be vulnerable and still-sensitive information will be prematurely disclosed AND all systems using legacy encryption technologies will possess NO reliable *confidentiality*. See Figure 2

The amount of risk will be more or less proportional to the *sensitivity* of the data whose shelf life has been compromised (prematurely ended) by quantum computers breaking the cryptography used to protect it.

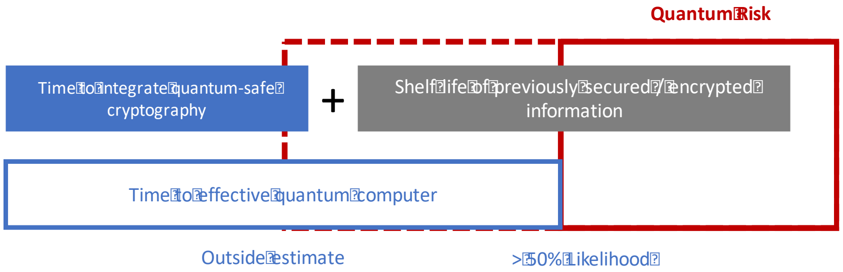
Quantum Risk
Time to integrate quantum-safe cryptography
+
Shelf life of previously secured / encrypted information
Time to effective quantum computer
Outside estimate
> 50% Likelihood

Figure 2: Quantum Risk equation

Quantum Risk scenarios

The risk of early and unauthorized information disclosure and confidentially breeches – “quantum risk” – differs by market and information type. Risk is typically a function of impact (sensitivity) and likelihood. In Table 4: Quantum Risk, we listed what we perceive to be the relative risks to four key market: Consumers, Businesses, Industry / Critical Infrastructure and finally Government and Military.

	Consumer	Business / Enterprise / Civilian Government	Industry / Critical Infrastructure	Public Safety / National Security
Information / Operational Technology	MEDIUM	HIGH	EXTREME	EXTREME

Table 4: Quantum Risk

Consumer IT quantum risk

MEDIUM

Consumers are facing quantum risks from their devices like smartphone, home computers and requirements to store and manage information like properties deeds, tax records and will.

The lifespan for most Consumer devices is 2 years or less. Upgrading or replacing Consumer devices is typically an easy and inexpensive undertaking, in fact many Consumer devices have an optimal lifespan of approximately 2 years, and warranties us usually only 1 year at most.

The shelf-life of data owned and managed by Consumer is commonly less than 5 years. Little about record Consumer retention of confidentiality is regulated with Consumers, there are definitely conventions and guidance from a range of professionals that every consumer should take into account.

As a result, it is unlikely that Consumers are at substantial risk today (in early 2018) from the advent of quantum computing and the deprecation of conventional encryption technology. See Figure 3: Consumer quantum risk

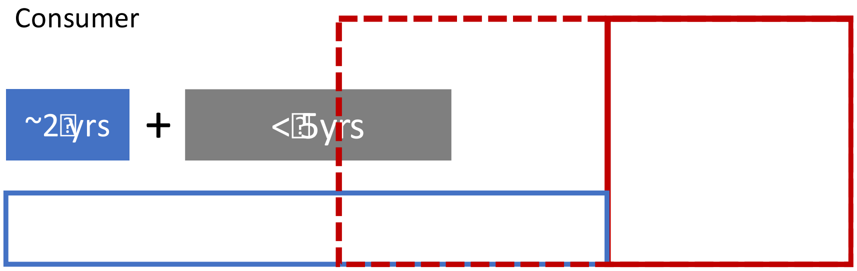

Figure 3: Consumer quantum risk

Business and Civilian Government IT quantum risk

HIGH

Business and civilian Government face quantum risks from the Information Technology (IT) that they use to conduct business such as mobile devices, desktops, servers (physical and virtual), dedicated networks and datacenters, cloud-based applications and services and communications over the internet with customers, partners, suppliers and regulators.

The lifespan of many business systems is regularly in the 4 to 6 year range, before refresh is planned and amortization has been completed; however, some business systems can remain in service much longer if they are supporting highly customized software. For instance, some banking and government systems are decades old. A major contributing factor to Business IT beyond the refresh intervals, it the additional time that selecting, testing, deploying and migrating to quantum-safe solutions will require.

The regulated shelf-life for much business information such as financial filings and business records is regularly over 7 years, however some data such as personally identifiable information can have lifespans related to the subject (the person) and therefore be indefinite from a business perspective.   Additionally, data such as artistic works with copyrights are protects for up to 70 years after the death of the "artist" and therefore have very long lifespans. Business and enterprise IT systems face many requirements to maintain confidentiality of information in areas ranging from personally identifiable information (privacy) to financial information to intellectual property, trade secrets, partner information and overall business strategy.

Business risk is considered HIGH at this time (early 2018) related to the advent of quantum computing and the deprecation of conventional encryption technology, because a conservative estimate of the time needed to retrofit existing IT solutions with quantum safe IT solution plus the minimum shelf-life of range of information managed by business and enterprise EXCEEDS the likely point at which convention encryption will be vulnerable to quantum threats.   See Figure 4: Business quantum risks.

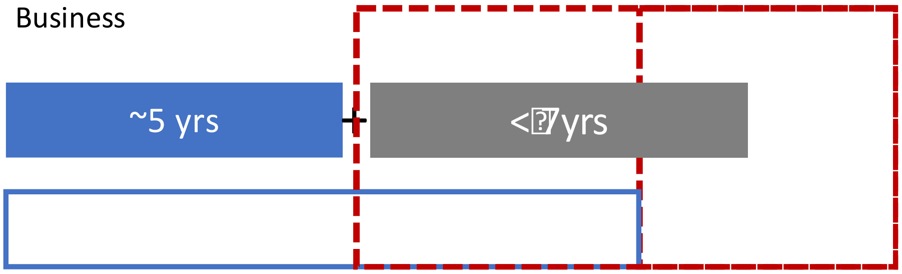

Figure 4: Business quantum risks

Industry / Critical Infrastructure.

EXTREME

Industry and Critical Infrastructure face quantum risks like Business, but also from Operationa Technology (OT), which they use to control manufacturing processes and cyber-physical interfaces.   This would include Industry IoT (IIoT) systems, Supervisory and Data Acquisition (SCADA) systems, Distributed Controls Systems (DCS) and Safety Systems which are typically distinct from other forms of control.

The lifespan of many OT systems is regularly in the 15 to 30 years of planned production or service-lifetime before amortization has been completed. For instance, Smart Cities, Energy, Transportation, Manufacturing and many utilities are already major users of OT. Many of these systems not only rely on the security of the communications links that support them, but also have direct connections to the business/Enterprise IT solutions and the Internet for remote management and supplier support.

The regulated shelf-life for much Industrial information such as production and safety records is regularly over 5 years.   Additionally, data such as intellectual property associated with production processes and recipes are the basis for their entire competitive advantage and while not regulated, possess substantial value to the firm.

Industry risk is considered EXTREME at this time (early 2018), primarily because of the time needed to retrofit existing OT solutions with quantum safe solutions.   This retrofit plus the minimum shelf-life of a range of information managed by Industry EXCEEDS the likely point at which conventional encryption will be vulnerable to quantum threats.   See Figure 5: Industrial / Critical Infrastructure quantum risk

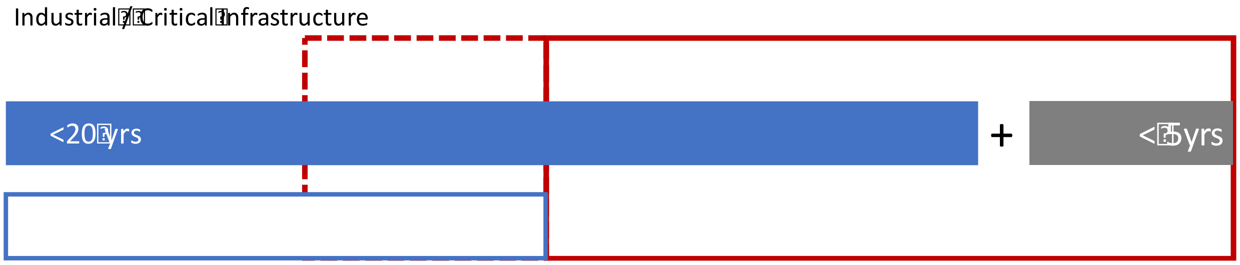

Figure 5: Industrial / Critical Infrastructure quantum risk

Public Safety and National Security

EXTREME

Public Safety and National Security information in Government face quantum risks, like Business, from the Information Technology (IT) that they use to conduct business such as mobile devices, desktops, servers (physical and virtual), dedicated networks and datacenters, cloud-based applications and services and communications over the internet with customers, partners, suppliers and regulators.

The lifespan of Public Safety and National Security IT systems may be similar to those of Business, in the 4 to 6 year range, before refresh is planned and amortization has been completed; however, some applications, platforms or infrastrcuture can remain in service much longer if they are supporting highly customized systems.

The shelf-life for Public Safety and National security information, such as policy deliberations, intelligence and sources, spending and resource allocations and troop/material records are frequently considered "classified" and carry a 25 year minimum lifespan in the United States and many NATO countries.

Government / Military risk is considered EXTREME at this time (early 2018) related to the advent of quantum computing and the deprecation of conventional encryption technology, primarily because the shelf-life of data for this grouping EXCEEDS the likely point at which convention encryption will be vulnerable to quantum threats.   See Figure 6: Public Safety / National Security quantum risk

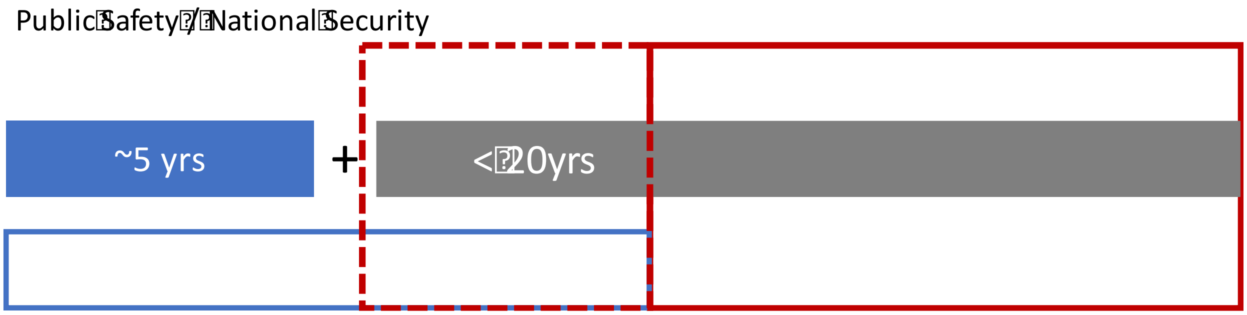

Figure 6: Public Safety / National Security quantum risk

Comments on the Cyber Security Framework.

As Per Section 3.2 of the Framework – Step 4: Conduct a Risk Assessment.

> […] *It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.*

We wish to focus out comments around this particular element and theme, which is repeated several times in the Framework.

Comment 1: The Framework and Roadmap are both silent on the merging criticality of cryptography ability in information systems.

Comment 2: The framework references several controls from NIST 800-53r4 which deal with cryptography, encryption and identity but are also silent on the important matters of cryptographic agility and quantum risk management.

The following is a mapping for the Framework to effected 800-53r4 sections CM-3, SC-12, SC-13

Function	Category	Subcategory	NIST Reference
Identify			
Protect	PR.IP – Info Protection Processes and Procedures	PR.IP (3) Configuration Change Control	CM-3
	PR.DS – Data Security	PR.DS(1) – Data At rest is protected	SC-12
		PR.DS (2) Data in transit is protected	SC-12
		PR.DS (5) – Protection against data leaks are implemented	SC-13
Detect	DE.CM – Continuous Monitoring	DE.CM (1) - The network is monitored to detect potential cybersecurity events	CM-3
Respond	NA	NA	NA
Recover	NA	NA	NA

Table 5: Framework sections addressing cryptography as a function of NIST 800-53r4 control mapping

Comment 3: The Framework Functions of “Respond” and “Recover” are silent about the role that cryptographic controls can aid in response and recovery. Clearly, Cryptographic Agility as described above can and does play a critical role in enterprise response and recovery to a growing list of vulnerabilities and increasing probability exploitation and therefore risk.

Comments on Roadmap for Improving Critical Infrastructure Cybersecurity

The Cyber Security Roadmap draft 1.1 listed the twelve topics below as “high priority areas for development”.

While “encryption” is discussed in several locations within the roadmap, most of the text is related to controls and issues that implement encryption rather than the management of encryption (or authentication technologies) itself.

1. Confidence Mechanisms
2. Cyber-Attack Lifecycle
3. Cybersecurity Workforce
4. Cyber Supply Chain Risk Management
5. Federal Agency Cybersecurity Alignment
6. Governance and Enterprise Risk Management
7. Identity Management
8. International Aspects, Impacts, and Alignment
9. Measuring Cybersecurity
10. Privacy Engineering
11. Referencing Techniques
12. Small Business Awareness and Resources

Comment 4: The Roadmap, which is supposed to guide future development of the Framework is also silent on the matter of *Cryptographic Agility* and *Quantum Risk Management*.

Recommendations

1) Introduce and discuss the topic of Cryptographic Agility within the Cyber Security Risk Management Framework, including the guidance related to the nature, composition and ownership of information assets that would benefit from agility

2) Introduce and discuss the topic of Quantum Risk Management within the Cyber Security Risk Management Framework, including the threats, vulnerabilities and risks associated with advent of quantum computing and conventional cryptographic algorithms

3) Include references to cryptographic controls in the “Respond” and “Recover” functions of the Framework, given the foundational properties of these controls for security across applications, platforms and networks.

4) Add quantum risk management as a item in the Roadmap for improving Critical Infrastructure Cybersecurity.

5) Acknowledge that the current version of 800-53r4 is silent or at best ambiguous on the matter of Cryptographic Agility and Quantum Risk management. The next update of NIST 800-53 should include guidance related to the nature of cryptographic agility and the specific needs for quantum risk management.

6) The Framework and Roadmap should provide a reference to current NIST efforts to standardize post-quantum algorithms and the security controls that will be impacted by revised cryptographic standards.

Appendix of NIST 800-53r4 Controls cited

Configuration Management (CM)

CM – 3 – Configuration Change Control

(6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT

The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management.

Supplemental Guidance: Regardless of the cryptographic means employed (e.g.,public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13.
References: NISTSpecialPublication800-128.

Systems and Communications Protections (SC)

SC-12 **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].
Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.
Control Enhancements:

CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).
CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes.

CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS

The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].

P1	**LOW** SC-12	**MOD** SC-12	**HIGH** SC-12 (1)

SC-13 CRYPTOGRAPHIC PROTECTION Control:

The information system implements in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
References: FIPSPublication140;Web:http://csrc.nist.gov/cryptval,http://www.cnss.gov.