Blended Critical Infrastructure Protection (CIP v1.1)

NIST Privacy Framework (NPF v1.0)

Security Control Baseline Analysis

Cyber Exome Ancestry Tool (CEAT) v1.0.0.5

By

Dr. Merrick S. Watchorn, DMIST, QSA Program Chair, Q-SRA

Mr. J. Aaron Bishop, QSA, Chief Executive Officer (CEO)

Contributing Author(s):

Dr. Keeper Layne Sharkey, Chair, Q-Chemical

Mrs. Michelle M. Watchorn, Chair, Q-Ethics

August 14, 2021

Abstract

Quantum Security Alliance (QSA) was formed to bring academia, industry, researchers, and US government entities together to identify, define, collaborate, baseline, standardize and protect sovereign countries, society, and individuals from the far-reaching impacts of Quantum Computing. The purpose of this document is to define the intersection of quantum, cybersecurity, privacy, and resiliency into a cohesive analysis document. Although, QSA believes that the impact of Quantum Computing and its inherit capabilities are a few years away, the transnational organizations and numerous nation states have already begun the thought process of how these can affect or influence strategic policy and privacy issues. According to Mavroeidis, Vasileios, Vishi, Kamer, Mateusz, Jøsang, and Audun, 2018) the differences between quantum and classical computing, challenges in quantum computing, quantum algorithms (Shor's and Grover's), public key encryption schemes affected, symmetric schemes affected, the impact on hash functions, and post quantum cryptography. Thus, the QSA determined the need to formulate a security control baseline that would address both critical infrastructure protection as defined by Executive Order, (EO 13800) Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure and privacy.

The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management Version 1.0 was released on January 2020 with an overlay mapping to the NIST Cybersecurity Framework. The QSA sought to define both quantum, critical infrastructure protection, and privacy risk into a unified analysis model to discover any hidden relationship. This document is a working document and will have several iterations soon as more discoveries are aligned into the unified analysis model. The QSA has begun the process of identifying key work roles that are affected in a quantum resistance environment and the protentional resiliency and criticality for FISMA and FIPS accreditation models. This paper will walk any interested party to understand his or her organizations future quantum-cyber-privacy profile in a Post-Quantum Encryption landscape. The influence of Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP) and Cognitive Computing are intentionally withheld from the approach to minimize a multi-thread and confusing dialog.

Blended Critical Infrastructure Protection (CIP v1.1)

NIST Privacy Framework (NPF v1.0)

Security Control Baseline Analysis

Cybersecurity Framework (CSF v1.1) dated January 15, 2018

Executive Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Like financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

To better address these risks, the Cybersecurity Enhancement Act of 20141 (CEA) statutorily updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." This formalized NIST's previous work developing Framework version 1.0 under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (February 2013), and provided guidance for future Framework evolution. The Framework that was developed under EO 13636 and continues to evolve according to CEA uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or

cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.

The Framework provides a common organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity. The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people domains. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). Applied to the people domain, the Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with the private sector and government agencies at all levels. As the Framework is put into greater practice, additional lessons learned will be integrated into future versions. This will ensure the Framework is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Expanded and more effective use and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing evolving guidance for individual organizations while increasing the cybersecurity posture of the Nation's critical infrastructure and the broader economy and society.

NIST Privacy Framework (NPF 1.0)

For more than two decades, the Internet and associated information technologies have driven unprecedented innovation, economic value, and improvement in social services. Many of these benefits are fueled by data about individuals that flow through a complex ecosystem. As a result, individuals may not be able to understand the potential consequences for their privacy as they interact with systems, products, and services. At the same time, organizations may not realize the full extent of these consequences for individuals, for society, or for their enterprises, which can affect their brands, their bottom lines, and their prospects for growth.

Following a transparent, consensus-based process including both private and public stakeholders to produce this voluntary tool, the National Institute of Standards and Technology (NIST) is publishing this Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework), to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy. The Privacy Framework can support organizations in:

•Building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;

•Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and

•Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators. Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions. Like building a house, where homeowners make layout and design choices while relying on a well-engineered foundation, privacy protection should allow for individual choices, as long as effective privacy risk mitigations are already engineered into products and services. The Privacy Framework—through a risk and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends, such as artificial intelligence and the Internet of Things.

Function

Identify (ID) - Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; Risk Management Strategy; and Supply Chain Risk Management.

Identify-P (ID-P) - Develop the organizational understanding to manage privacy risk for individuals arising from data processing. The activities in the Identify-P Function are foundational for effective use of the Privacy Framework. Inventorying the circumstances under which data are processed, understanding the privacy interests of individuals directly or indirectly served or affected by an organization, and conducting risk assessments enable an organization to understand the business environment in which it is operating and identify and prioritize privacy risks.

Critical Infrastructure Protection Categories:

Asset Management (ID.AM) - The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.

Categories-Sub:

ID.AM-1 - Physical devices and systems. Within the organization are inventoried. NIST Control(s): CM-8, PM-5

ID.AM-2 - Software platforms and applications within the organization are inventoried. NIST Control(s): CM-8, PM-5

ID.AM-3 - Organizational communication and data flows are mapped. NIST Control(s): AC-4, CA-3, CA-9, PL-8

ID.AM-4 - External information systems are catalogued. NIST Control(s): AC-20, SA-9

ID.AM-5 - Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value. NIST Control(s): CP-2, RA-2, SA-14, SC-6

ID.AM-6 - Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. NIST Control(s): CP-2, PS-7, PM-11

Privacy Categories:

Business Environment (ID.BE) - The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Categories-Sub:

ID.BE-1 - The organization's role in the supply chain is identified and communicated. NIST Control(s): CP-2, SA-12

ID.BE-2 - The organization's place in critical infrastructure and its industry sector is identified and communicated. NIST Control(s): PM-8

ID.BE-3 - Priorities for organizational mission, objectives, and activities are established and communicated. NIST Control(s): PM-11, SA-14

ID.BE-4 - Dependencies and critical functions for delivery of critical services are established. NIST Control(s): CP-8, PE-9, PE-11, PM-8, SA-14

ID.BE-5 - Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations). NIST Control(s): CP-2, CP-11, SA-13, SA-14

Privacy Categories:

Governance (ID.GV) - The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Categories-Sub:

ID.GV-1 - Organizational information security policy is established. NIST Control(s): -1 controls from all families

ID.GV-2 - Information security roles & responsibilities are coordinated and aligned with internal roles and external partners. NIST Control(s): PS-7, PM-1, PM-2

ID.GV-3 - Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. NIST Control(s): -1 controls from all families (except PM-1)

ID.GV-4 - Governance and risk management processes address cybersecurity risks. NIST Control(s): SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

Privacy Categories:

Risk Assessment (ID.RA) - The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Categories-Sub:

ID.RA-1 - Asset vulnerabilities are identified and documented. NIST Control(s): CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

ID.RA-2 - Cyber threat intelligence is received from information sharing forums and sources. NIST Control(s): SI-5, PM-15, PM-16

ID.RA-3 - Threats, both internal and external, are identified and documented. NIST Control(s): RA-3, SI-5, PM-12, PM-16

ID.RA-4 - Potential business impacts and likelihoods are identified. NIST Control(s): RA-2, RA-3, SA-14, PM-9, PM-11

ID.RA-5 - Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. NIST Control(s): RA-2, RA-3, PM-16

ID.RA-6 - Risk responses are identified and prioritized. NIST Control(s): PM-4, PM-9

Privacy Categories:

Risk Management Strategy (ID.RM) - The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Categories-Sub:

ID.RM-1 - Risk management processes are established, managed, and agreed to by organizational stakeholders. NIST Control(s): PM-9

ID.RM-2 - Organizational risk tolerance is determined and clearly expressed. NIST Control(s): PM-9

ID.RM-3 - The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis. NIST Control(s): SA-14, PM-8, PM-9, PM-11

Privacy Categories:

Supply Chain Risk Management (ID.SC) - The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Categories-Sub:

ID.SC-1 - Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. NIST Control(s): SA-9, SA-12, PM-9

ID.SC-2 - Identify, prioritize and assess suppliers and third-party partners of information systems, components and services using a cyber supply chain risk assessment process. NIST Control(s): RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

ID.SC-3 - Suppliers and third-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan. NIST Control(s): SA-9, SA-11, SA-12, PM-9

ID.SC-4 - Suppliers and third-party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted. NIST Control(s): AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12

ID.SC-5 - Response and recovery planning and testing are conducted with suppliers and third-party providers. NIST Control(s): CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Privacy Categories:

Function

Protect (PR) - Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Govern-P (GV-P) - Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. The Govern-P Function is similarly foundational but focuses on organizational-level activities such as establishing organizational privacy values and policies, identifying legal/regulatory requirements, and understanding organizational risk tolerance that enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Critical Infrastructure Protection Categories:

Identity Management, Authentication and Access Control (PR.AC) - Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Categories-Sub:

PR.AC-1 - Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. NIST Control(s): AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

PR.AC-2 - Physical access to assets is managed and protected. NIST Control(s): PE-2, PE-3, PE-4, PE-5, PE-6, PE-8

PR.AC-3 - Remote access is managed. NIST Control(s): AC-1, AC-17, AC-19, AC-20, SC-15

PR.AC-4 - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. NIST Control(s): AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24

PR.AC-5 - Network integrity is protected, incorporating network segregation where appropriate. NIST Control(s): AC-4, AC-10, SC-7

PR.AC-6 - Identities are proofed and bound to credentials and asserted in interactions when appropriate. NIST Control(s): AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

PR.AC-7 - Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). NIST Control(s): AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

Privacy Categories:

Awareness and Training (PR.AT) - The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Categories-Sub:

PR.AT-1 - Users are informed and trained. NIST Control(s): AT-2, PM-13

PR.AT-2 - Privileged users understand roles and responsibilities. NIST Control(s): AT-3, PM-13

PR.AT-3 - Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities. NIST Control(s): PS-7, SA-9, SA-16

PR.AT-4 - Senior executives understand roles and responsibilities. NIST Control(s): AT-3, PM-13

PR.AT-5 - Physical and information security personnel understand roles and responsibilities. NIST Control(s): AT-3, IR-2, PM-13

Privacy Categories:

Data Security (PR.DS) - Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Categories-Sub:

PR.DS-1 - Data-at-rest is protected. NIST Control(s): MP-8, SC-12, SC-28

PR.DS-2 - Data-in-transit is protected. NIST Control(s): SC-8, SC-11, SC-12

PR.DS-3 - Assets are formally managed throughout removal, transfers, and disposition. NIST Control(s): CM-8, MP-6, PE-16

PR.DS-4 - Adequate capacity to ensure availability is maintained. NIST Control(s): AU-4, CP-2, SC-5

PR.DS-5 - Protections against data leaks are implemented. NIST Control(s): AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

PR.DS-6 - Integrity checking mechanisms are used to verify software, firmware, and information integrity. NIST Control(s): SC-16, SI-7

PR.DS-7 - The development and testing environment(s) are separate from the production environment. NIST Control(s): CM-2

PR.DS-8 - Integrity checking mechanisms are used to verify hardware integrity. NIST Control(s): SA-10, SI-7

Privacy Categories:

Information Protection Processes and Procedures (PR.IP) - Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Categories-Sub:

PR.IP-1 - A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality). NIST Control(s): CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

PR.IP-2 - A System Development Life Cycle to manage systems is implemented. NIST Control(s): PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17

PR.IP-3 - Configuration change control processes are in place. NIST Control(s): CM-3, CM-4, SA-10

PR.IP-4 - Backups of information are conducted, maintained, and tested periodically. NIST Control(s): CP-4, CP-6, CP-9

PR.IP-5 - Policy and regulations regarding the physical operating environment for organizational assets are met. NIST Control(s): PE-10, PE-12, PE-13, PE-14, PE-15, PE-18

PR.IP-6 - Data is destroyed according to policy. NIST Control(s): MP-6

PR.IP-7 - Protection processes are continuously improved. NIST Control(s): CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

PR.IP-8 - Effectiveness of protection technologies is shared with appropriate parties. NIST Control(s): AC-21, CA-7, SI-4

PR.IP-9 - Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. NIST Control(s): CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17

PR.IP-10 - Response and recovery plans are tested. NIST Control(s): CP-4, IR-3, PM-14

PR.IP-11 - Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). NIST Control(s): PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

PR.IP-12 - A vulnerability management plan is developed and implemented. NIST Control(s): RA-3, RA-5, SI-2

Privacy Categories:

Maintenance (PR.MA) - Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Categories-Sub:

PR.MA-1 - Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools. NIST Control(s): MA-2, MA-3, MA-5, MA-6

PR.MA-2 - Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. NIST Control(s): MA-4

Privacy Categories:

Protective Technology (PR.PT) - Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Categories-Sub:

PR.PT-1 - Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. NIST Control(s): AU Family

PR.PT-2 - Removable media is protected and its use restricted according to policy. NIST Control(s): MP-2, MP-3, MP-4, MP-5, MP-7, MP-8

PR.PT-3 - The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. NIST Control(s): AC-3, CM-7

PR.PT-4 - Communications and control networks are protected. NIST Control(s): AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

PR.PT-5 - Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations). NIST Control(s): CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Privacy Categories:

Function

Detect (DE) - Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Control-P (CT-P) - Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks. The Control-P function considers data processing management from the standpoint of both organizations and individuals.

Critical Infrastructure Protection Categories:

Anomalies and Events (DE.AE) - Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Categories-Sub:

DE.AE-1 - A baseline of network operations and expected data flows for users and systems is established and managed. NIST Control(s): AC-4, CA-3, CM-2, SI-4

DE.AE-2 - Detected events are analyzed to understand attack targets and methods. NIST Control(s): AU-6, CA-7, IR-4, SI-4

DE.AE-3 - Event data are collected and correlated from multiple sources and sensors. NIST Control(s): AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

DE.AE-4 - Impact of events is determined. NIST Control(s): CP-2, IR-4, RA-3, SI-4

DE.AE-5 - Incident alert thresholds are established. NIST Control(s): IR-4, IR-5, IR-8

Privacy Categories:

Security Continuous Monitoring (DE.CM) - The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Categories-Sub:

DE.CM-1 - The network is monitored to detect potential cybersecurity events. NIST Control(s): AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

DE.CM-2 - The physical environment is monitored to detect potential cybersecurity events. NIST Control(s): CA-7, PE-3, PE-6, PE-20

DE.CM-3 - Personnel activity is monitored to detect potential cybersecurity events. NIST Control(s): AC-2, AU-12, AU-13, CA-7, CM-10, CM-11

DE.CM-4 - Malicious code is detected. NIST Control(s): SI-3, SI-8

DE.CM-5 - Unauthorized mobile code is detected. NIST Control(s): SC-18, SI-4, SC-44

DE.CM-6 - External service provider activity is monitored to detect potential cybersecurity events. NIST Control(s): CA-7, PS-7, SA-4, SA-9, SI-4

DE.CM-7 - Monitoring for unauthorized personnel, connections, devices, and software is performed. NIST Control(s): AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4

DE.CM-8 - Vulnerability scans are performed. NIST Control(s): RA-5

Privacy Categories:

Detection Processes (DE.DP) - Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Categories-Sub:

DE.DP-1 - Roles and responsibilities for detection are well defined to ensure accountability. NIST Control(s): CA-2, CA-7, PM-14

DE.DP-2 - Detection activities comply with all applicable requirements. NIST Control(s): AC-25, CA-2, CA-7, SA-18, SI-4, PM-14

DE.DP-3 - Detection processes are tested. NIST Control(s): CA-2, CA-7, PE-3, SI-3, SI-4, PM-14

DE.DP-4 - Event detection information is communicated to appropriate parties. NIST Control(s): AU-6, CA-2, CA-7, RA-5, SI-4

DE.DP-5 - Detection processes are continuously improved. NIST Control(s): CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Privacy Categories:

Function

Respond (RS) - Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Communicate-P (CM-P) - Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks. The Communicate-P function recognizes that both organizations and individuals may need to know how data are processed in order to manage privacy risk effectively.

Critical Infrastructure Protection Categories:

Response Planning (RS.RP) - Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity incidents.

Categories-Sub:

RS.RP-1 - Response plan is executed during or after an incident. NIST Control(s): CP-2, CP-10, IR-4, IR-8

Privacy Categories:

Communications (RS.CO) - Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Categories-Sub:

RS.CO-1 - Personnel know their roles and order of operations when a response is needed. NIST Control(s): CP-2, CP-3, IR-3, IR-8

RS.CO-2 - Incidents are reported consistent with established criteria. NIST Control(s): AU-6, IR-6, IR-8

RS.CO-3 - Information is shared consistent with response plans. NIST Control(s): CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4

RS.CO-4 - Coordination with stakeholders occurs consistent with response plans. NIST Control(s): CP-2, IR-4, IR-8

RS.CO-5 - Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. NIST Control(s): SI-5, PM-15

Privacy Categories:

Analysis (RS.AN) - Analysis is conducted to ensure adequate response and support recovery activities.

Categories-Sub:

RS.AN-1 - Notifications from detection systems are investigated. NIST Control(s): AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

RS.AN-2 - The impact of the incident is understood. NIST Control(s): CP-2, IR-4

RS.AN-3 - Forensics are performed. NIST Control(s): AU-7, IR-4

RS.AN-4 - Incidents are categorized consistent with response plans. NIST Control(s): CP-2, IR-4, IR-5, IR-8

RS.AN-5 - Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers). NIST Control(s): SI-5, PM-15

Privacy Categories:

Mitigation (RS.MI) - Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

Categories-Sub:

RS.MI-1 - Incidents are contained. NIST Control(s): IR-4

RS.MI-2 - Incidents are mitigated. NIST Control(s): IR-4

RS.MI-3 - Newly identified vulnerabilities are mitigated or documented as accepted risks. NIST Control(s): CA-7, RA-3, RA-5

Privacy Categories:

Improvements (RS.IM) - Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Categories-Sub:

RS.IM-1 - Response plans incorporate lessons learned. NIST Control(s): CP-2, IR-4, IR-8

RS.IM-2 - Response strategies are updated. NIST Control(s): CP-2, IR-4, IR-8

Privacy Categories:

Function

Recover (RC) - Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Protect-P (PR-P) - Develop and implement appropriate data processing safeguards. The Protect-P Function covers data protection to prevent cyber security-related privacy events, the overlap between privacy and cyber security risk management.

Critical Infrastructure Protection Categories:

Recovery Planning (RC.RP) - Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents.

Categories-Sub:

RC.RP-1 - Recovery plan is executed during or after a cybersecurity incident. NIST Control(s): CP-10, IR-4, IR-8

Privacy Categories:

Improvements (RC.IM) - Recovery planning and processes are improved by incorporating lessons learned into future activities.

Categories-Sub:

RC.IM-1 - Recovery plans incorporate lessons learned. NIST Control(s): CP-2, IR-4, IR-8

RC.IM-2 - Recovery strategies are updated. NIST Control(s): CP-2, IR-4, IR-8

Privacy Categories:

Communications (RC.CO) - Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Categories-Sub:

RC.CO-1 - Public relations are managed. NIST Control(s):

RC.CO-2 - Reputation after an event is repaired. NIST Control(s):

RC.CO-3 - Recovery activities are communicated to internal stakeholders and executive and management teams. NIST Control(s): CP-2, IR-4

Privacy Categories:

Quantum Computing (QC)

Critical Infrastructure Protection (CIP)

Privacy Framework

Blended Security Control Baseline

The Cyber Order of Operations and Methodology (COoOM) is a multi-sided angled approach to cybersecurity, which requires a complexity understanding of some simple decision points and an order of decision-making that is much like a choose your own adventure reading book from the early 80's. The intent of this presentation is to demonstrate the level of pre-analysis required to achieve a semblance of a repeatable process with an embedded outcome process based on the response and needs of the individual, organization, program, or service. Thus, each organization should consider building a Cyber Order of Operations Method (COoOM) to achieve their desired security posture. Thanks to Mr. J. Aaron Bishop for providing an excellent argument point stay tuned as QSA continues to research into finding logic, reason, method, and analysis of this change for the United States and all sub-contracting organizations that support them. The NIST SP 800-53 Rev. 5 was used to build a stronger understanding of the baseline from the COoOM perspective. The COoOM angles for this analysis was 22 and the entire index count of the NIST SP 800-53 Rev. 5 has 1007 active controls. During the conversion process 13 security controls were found to be removed in Rev. 5 from NIST SP 800-53 Rev. 4.

The blending of the privacy and Critical Infrastructure Protection framework resulted in 320 control selected or totalControls: (320 / 1007) * 100 = 31.78% of all active controls. The final step was to document controls that had privacy and CIP element responsibility for FISMA, Privacy Act or known legal frameworks to discover additional control considerations. A simple summary for the selected security control baselines is provided for external validation and justification of process.

1. NIST SP 800-53 Rev. 5: (320 / 1007) * 100 = 31.78%
2. CEAT NIST SP 800-53 R5 - Confidentiality: (166 / 492) * 100 = 33.74%
3. CEAT NIST SP 800-53 R5 - Integrity: (201 / 596) * 100 = 33.72%
4. CEAT NIST SP 800-53 R5 - Availability: (109 / 307) * 100 = 35.50%
5. CEAT NIST SP 800-53 R5 - Criticality: (77 / 198) * 100 = 38.89%
6. NIST SP 800-53 R5 - APT: (11 / 62) * 100 = 17.74%
7. NIST SP 800-53 R5 - Assurance: (137 / 425) * 100 = 32.24%
8. NIST SP 800-53 R5 - CIP: (191 / 233) * 100 = 81.97%
9. NIST SP 800-53 R5 - Discretionary: (24 / 62) * 100 = 38.71%
10. NIST SP 800-53 R5 - Implemented O: (218 / 606) * 100 = 35.97%
11. NIST SP 800-53 R5 - Implemented O/S: (33 / 150) * 100 = 22.00%
12. NIST SP 800-53 R5 - Implemented S: (69 / 250) * 100 = 27.60%
13. CEAT NIST SP 800-53 R5 - Insider Threat: (22 / 85) * 100 = 25.88%
14. NIST SP 800-53 R5 - Joint: (60 / 97) * 100 = 61.86%
15. NIST SP 800-53 R5 - Management: (71 / 228) * 100 = 31.14%
16. NIST SP 800-53 R5 - Operational: (122 / 398) * 100 = 30.65%
17. NIST SP 800-53 R5 - Privacy: (79 / 96) * 100 = 82.29%
18. NIST SP 800-53 R5 - Required: (42 / 44) * 100 = 95.45%
19. NIST SP 800-53 R5 - Situationally Required: (13 / 19) * 100 = 68.42%
20. NIST SP 800-53 R5 - SCRM: (126 / 224) * 100 = 56.25%
21. NIST SP 800-53 R5 - Technical: (127 / 381) * 100 = 33.33%
22. CEAT NIST SP 800-53 R5 - Legal: (127 / 158) * 100 = 80.38%