3.4.2.3 Network Vulnerabilities The MITRE Corporation’s Common Vulnerabilities and Exposures database (CVE) lists more than 85,000 vulnerabilities that can affect web servers, Structured Query Language (SQL) servers, DNS servers, firewalls, routers, and other network components (see https://cve.mitre.org). These include vulnerabilities that can result in denial of service, code execution, overflow, cross-site scripting, directory traversal, process bypass, unauthorized gaining of information, SQL injection, file inclusion, memory corruption, cross-site request forgery, and http response splitting. Many of the vulnerabilities are operating system or application-based. Others are protocol based (e.g., vulnerabilities inherent in IP22, TLS, DNS23, Border Gateway Protocol (BGP) 24, SMTP and other network protocols). As in the case of client system vulnerabilities, NIST’s NVD (https://nvd.nist.gov) is a frequently updated source of vulnerabilities that affect network servers. 3.4.3 Risk Risks are examined from the point of view of consequences of vulnerabilities being exploited. Some examples of these consequences include legal liability, consequences of failure to comply with regulations, confidentiality breaches, loss of productivity, and damage to organizational reputation. ♣ New and existing regulations are forcing organizations to keep a record of their emails and to protect their employee and customer privacy. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires health care institutions to keep a record of their email communications and secure confidentiality of information. In the new Internal Revenue Service (IRS) regulation Circular 230, the IRS requires tax advisors to add an email disclaimer to any emails including tax advice, expressly stating that the opinion cannot be relied upon for penalty purposes. The U.S. Securities and Exchange Commission and Gramm-Leach-Bliley Act impose similar duties on financial institutions. Steep penalties can apply to those organizations that do not comply with their industry’s regulations. In a case lasting from 2000 until 2005, a wellknown financial institution was recently forced to pay 20 million dollars in penalties by the Securities and Exchange Commission for not diligently searching for email backup tapes and overwriting multiple backup tapes. ♣ Most confidentiality breaches occur from within the company. These breaches can be accidental, but they can also be intentional. 22 RFC 791, Internet Protocol 23 RFC 1034, Domain Names - Concepts and Facilities 24 RFC 4271, A Border Gateway Protocol 4 (BGP-4) NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 15 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. ♣ With respect to legal liability, organizations are generally held responsible for all the information transmitted on or from their system, so inappropriate emails sent on the company network can result in multi-million dollar penalties. ♣ Employees sending personal emails and sifting through spam mail can cause major loss of productivity.25 ♣ Even just a badly written email, or an email containing unprofessional remarks will cause the recipient to gain a bad impression of the company that the sender is representing. Fraudulent email attributable to an organization can do far more damage to an organization’s reputation, both in terms of the response elicited and in terms of loss of confidence in the cybersecurity reliability of the organization. ♣ Another example of consequence may be damage to the perceived value of an organization, to be distinguished from organizational reputation, which is more about the habits or characteristics of a particular organization.26 A number of cybersecurity actions are recommended to reduce these risks. The Framework Core identified in NIST’s Cybersecurity Framework is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. 3.4.4 Cybersecurity Framework Functions, Categories, and Subcategories Addressed by the Project NIST’s Cybersecurity Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities—including sector coordinating structures, associations, and organizations—can use the Cybersecurity Framework for different purposes, including the creation of common profiles. As stated 25 Current spam filtering solutions consist of some sort of filtering at the network or the PC level, and they do not reveal the details of the sender without looking up the source. It takes some work for the recipient. This will always put us one step behind our adversaries. DNS provides the necessary Internet-wide scaling. 26 Please see: https://www.wired.com/2016/10/security-news-week-verizon-reportedly-wants-1-billion-discountyahoo-deal/ and http:/nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports/. ”The discount is being pushed because it feels Yahoo’s value has been diminished,” sources said. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 16 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. above, the Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References. ♣ Functions organize basic cybersecurity activities at their highest level. These Functions are: Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services. ♣ Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.” ♣ Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.” ♣ Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process. This project supported the Cybersecurity Framework’s Protect, Detect, and Respond Functions. Applicability to specific Functions, Categories, and Subcategories is described in the following paragraphs. 3.4.4.1 Protect The Protect Function develops and implements the appropriate safeguards needed to ensure delivery of critical infrastructure services. This Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function addressed by the project include: Access Control, Data Security, and Protective Technology. 1. Access Control (PR.AC) a. PR.AC-1 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 17 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. The PR.AC-1 subcategory under Access Control supports identities and credentials being managed for authorized devices and users. The security platform resulting from the project supports effective management of the credentials associated with the addresses from which email purportedly originates and the integrity of the user identities associated with the email. The original design of the DNS did not include security; instead, it was designed to be a scalable distributed system. DNSSEC and DANE attempt to add security, while maintaining backward compatibility with the existing DNS. DNSSEC was designed to protect applications (and caching resolvers serving those applications) from using forged or manipulated DNS data. All answers from DNSSEC protected zones are cryptographically signed (i.e., digital signature over DNS data). By checking the digital signature, a DNS resolver is able to determine whether the information is authentic (i.e., unmodified and complete) and is served on an authoritative DNS server. While protecting IP addresses is the immediate concern for many users, DNSSEC can protect any data published in the DNS, including text records or mail exchange (MX) records, and can be used to bootstrap other security systems that publish references to cryptographic certificates stored in the DNS. All DNSSEC responses contain signed DNS data. DNSSEC signature validation allows the use of potentially untrustworthy parties if (for example) the mail server is using a selfsigned certificate. The protocol permits configuration of systems to accept messages whether or not they are digitally signed. The security platform developed under the project permits email clients and transfer agents to be configured to send email messages to only servers whose DNS entries are digitally signed. At the client systems level (e.g., Outlook, Postfix, Thunderbird), digital signature of the mail messages themselves can also be applied on a user-to-user basis. In the user-to-user case, the signature provides assurance of the integrity of the identity of the sender rather than just the identity of the DNS zone(s) associated with the sender. b. PR.AC-5 The PR.AC-5 subcategory under Access Control supports protection of network integrity by incorporating network segregation where appropriate. The project does not specifically employ network segregation principles. However, it does support network integrity by providing operationally feasible mechanisms for preventing connections or message delivery to sources that do not implement a specified set of DNS security extensions. Rigorous adherence to a minimum security configuration can enforce effective isolation of a network from entities that do not conform to the network’s security requirements. NIST SP 800-53, referred to by this subcategory, requires information systems to enforce approved authorizations for controlling the flow of NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 18 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. information within systems and between interconnected systems (AC-4, Information Flow Enforcement). 2. Data Security (PR.DS) The Protect Function’s Data Security Category supports an outcome in which information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. The project demonstrates a capability to provide source and content integrity protection by employing digital signature of messages and confidentiality protection by encrypting messages. a. PR.DS-1 The PR.DS-1 subcategory under Data Security supports protection of data at rest. The user-to-user digital signature capability demonstrated by the project can provide an ability to verify the source and content integrity of locally stored email messages where the digital signature is stored with the rest of the message. This supports integrity protection for data-at-rest. b. PR.DS-2 The PR.DS-2 subcategory under Data Security supports protection of data in transit. In addition to user-to-user digital signature of email, the project demonstrates a capability to provide source and content integrity protection to data-in-transit. The demonstration accomplishes this by employing server-to-server confidentiality protection to data-in-transit by employing server-to-server encryption. c. PR.DS-6 The PR.DS-6 subcategory under Data Security supports use of integrity checking mechanisms to verify software, firmware, and information integrity. The digital signature of email demonstrated by the project’s security platform supports automatic integrity checking of information communicated in email messages. DNSSEC and DANE protect the integrity of address information. 3. Protective Technology (PR.PT) a. PR.PT-4 The PR.PT-4 subcategory under Protective Technology supports protection of communications and control networks. The project demonstrates a capability to provide source and content integrity protection by employing digital signature of communications and confidentiality protection by encrypting communications. The project’s demonstration of DNSSEC and DANE protocols also supports communications NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 19 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. and control network integrity. It does this by demonstrating operationally feasible mechanisms for refusing connections to or message delivery from sources that do not implement a specified set of DNS security extensions. Rigorous adherence to a minimum security configuration can be used to enforce isolation of networks from entities that do not conform to the network’s security requirements. 3.4.4.2 Detect The Detect Function develops and implements the appropriate activities needed to identify in a timely manner the occurrence of a cybersecurity event. Examples of outcome categories within this function addressed by the project include Security Continuous Monitoring and Detection Processes. 1. Security Continuous Monitoring (DE.CM) The Security Continuous Monitoring Category supports an outcome in which information systems and assets are monitored at discrete intervals to identify cybersecurity events and to verify the effectiveness of protective measures. While not a classic example of continuous monitoring, the project’s platform has the ability to automatically check all DNS responses for correct digital signatures. a. DE.CM-1 The DE.CM-1 subcategory under Security Continuous Monitoring supports monitoring of networks to detect potential cybersecurity events. While not a classic example of continuous monitoring, the demonstrated capability of the project’s platform to automatically check all inbound DNS responses for valid digital signatures permits identification of attempts to spoof systems using bogus DNS data. Automatic signing and signature validation for email permits continuous checking for false sender identities and modification of message content. NIST SP 800-53, referred to by this subcategory, requires monitoring of inbound and outbound communications traffic for unauthorized conditions (SI-4 [4]). Validation of DNS addresses supports this requirement. b. DE.CM-6 The DE.CM-6 subcategory under Security Continuous Monitoring supports monitoring of external service provider activity to detect potential cybersecurity events. While not a classic example of continuous monitoring, the demonstrated capability of the project’s platform to automatically check all inbound DNS responses for valid digital signatures permits detection of attempts by invalid service providers (e.g., bogus Certificate Authorities or Mail Transfer Agents) to spoof users’ systems (including manin-the-middle attacks). NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 20 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 2. Detection Processes (DE.DP) The Detection Processes Category supports an outcome in which detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. a. DE.DP-4 The DE.DP-4 subcategory under Detection Processes supports the communication of event detection information to appropriate parties. One of the shortcomings of most DNSSEC and DANE mechanisms is that they abort delivery of messages to destinations whose DNSSEC signature checks fail to validate and do not provide any indication that failure is due to an invalid signature. This usually results in numerous retransmissions and consequent performance degradation or possible crashes. The project’s platform includes notifications of DNS signature failures to mail agents in its DNS resolvers in order to prevent consequent performance degradation. This communication of detection information has the potential to mitigate one of the primary impediments to private sector adoption of DNSSEC. 3.4.4.3 Respond The Respond Function develops and implements the appropriate activities to take action regarding a detected cybersecurity event. This Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome categories within this function addressed by the project include: Response Planning, Communications, and Mitigation. 1. Response Planning (RS.RP) The Response Planning Category supports an outcome in which response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events. a. RS.RP-1 The RS.RP-1 subcategory under Response Planning supports execution of a response plan during or after an event. Inclusion of DNS and email security considerations in planning for connection of systems to the Internet will necessarily include responses to detection of invalid digital signatures. This includes security flagging of connections and messages and/or refusing connections and delivery of messages. Concurrent with detection of validation failure, these responses are demonstrated by the project’s platform. 2. Communications (RS.CO) NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 21 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. The Respond Communications Category requires response activities to be coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. a. RS.CO-2 The RS.CO-2 subcategory under Communications supports reporting of events consistent with established criteria. As stated under DE.DP-4, one of the shortcomings of most DNSSEC and DANE mechanisms is that they abort delivery of messages to destinations whose DNSSEC signature checks fail but do not provide any indication that the failure is due to an invalid signature. To prevent consequent performance degradation, the project’s platform includes notifications of DNSSEC signature failures to mail agents in its DNS resolvers. This communication of detection information has the potential to mitigate one of the primary impediments to private sector adoption of DNSSEC. It also provides a mechanism that can be exploited to provide information involving failures of DNSSEC signature checks to external stakeholders. 3. Mitigation (RS.MI) The Response Mitigation Category requires activities to be performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. a. RS.MI-1 The RS.MI-1 subcategory under Mitigation supports containment of incidents. Implementation of the project’s platform will contain the effects of incidents because any spoofing attempts or modified email will be detected and contained before they have a chance to negatively impact any organizational systems.27 b. RS.MI-2 The RS.MI-2 subcategory under Mitigation supports mitigation of incidents. The project demonstrates user-to-user digital signature of messages. Retention of their digital signatures with stored messages permits later determination of whether the messages have been modified in storage. This can be a mitigating factor in the case of incidents that involve introduction of fraudulent information into email records. The project’s demonstration of server-to-server encryption provides confidentiality protection for data-in-transit. This confidentiality protection can serve as a mitigating factor in the 27 Note that if a system is subverted, a lot of assumed security goes out the window. A subverted sending MTA could still be seen as valid by receivers, for example. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 22 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. case of incidents involving unauthorized access to messages captured by network devices that sit between the sender’s and recipient’s mail servers. 3.4.5 Cybersecurity References Directly Tied to Those Cybersecurity Framework Categories and Subcategories Addressed by the Project The following security references were followed in accepting components for the project’s platform, designing the platform, conducting demonstrations of the platform, and documenting the platform. The Framework Functions, Categories, and Subcategories addressed by these references are listed for each reference. While many of the references were written as standards and guidelines to be applied to federal government agencies, their recommendations may also be applied in the private sector as best practices that support the Cybersecurity Framework. Those Subcategories addressed by the platform are in boldface. 1. Security Requirements for Cryptographic Modules, Federal Information Processing Standard (FIPS) 140-2, May 2001. https://doi.org/10.6028/NIST.FIPS.140-2. FIPS 140-2 provides a standard that is required to be used by Federal organizations when these organizations specify that cryptographic-based security systems be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. All cryptographic components employed by the Federal government outside the national security community, including NCCoE security platforms that employ cryptography, must conform to FIPS 140-2. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. Within the context of the Cybersecurity Framework, FIPS 140-2 provides standards for “Protection” to be provided by cryptographic modules (PR.AC-2, PR.AC-4, PR.DS-1, PR.DS-2, PR.DS-5, PR.DS-6, PR.IP-3, and PR.PT-4) and “Detection” of failures or other exception conditions that might affect the protection afforded to systems by cryptographic modules (DE.CM-1, DE.CM-2, and DM.DP-3). NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 23 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 2. Guide for Applying the Risk Management Framework to Federal Information Systems: A security Lifecycle Approach, NIST SP 800-37 Rev. 1, Joint Task Force Transformation Initiative; February 2010 with updates as of June 5, 2014. https://doi.org/10.6028/NIST.SP.800-37r1. SP 800-37 Rev. 1 provides guidelines for applying the Risk Management Framework (RMF) to federal information systems. Systems to which the RMF is to be applied include NCCoE use case and block activities. The RMF promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes; provides senior leaders with the necessary information to make costeffective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions; and integrates information security into the enterprise architecture and development life cycle. Applying the RMF within enterprises links management processes at the information system level to management processes at the organization level through a risk executive (function) and establishes lines of responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls). The six-step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. With respect to the Cybersecurity Framework, SP 800-37 assumes that system components, business environment and governance structure have been identified. The risk assessment that underlies categorization is based on the assumed understanding of these factors. SP 800-37 also focuses on impacts of security incidents rather than on threats that take advantage of system vulnerabilities to create those impacts. The control selection, control implementation, and system authorization recommendations of SP 800-37 do not map directly to the Cybersecurity Framework. However, SP 800-37 does provide recommendations relevant to Identify (ID.RA-5, ID.RA-6, ID.RM 1, and ID.RM-2 in Section 3.1), Protect (PR.IP-3, and PR.IP-7 in Sections 3.4 and 3.6), and Detect, (DE.AE-5 and DE.CM-1 in Section 3.6) elements of the Cybersecurity Framework. 3. Guidelines on Electronic Mail Security; NIST SP 800-45 Ver. 2; Tracy, Jansen, Scarfone, Butterfield; February 2007. https://doi.org/10.6028/NIST.SP.800-45ver2. SP 800-45 provides guidelines intended to assist organizations in installing, configuring, and maintaining secure mail servers and mail clients. Specifically, the publication discusses in detail: a. email standards and their security implications b. email message signing and encryption standards c. the planning and management of mail servers NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 24 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. d. securing the operating system underlying a mail server e. mail server application security f. email-content filtering g. email-specific considerations in the deployment and configuration of network protection mechanisms, such as firewalls, routers, switches, and intrusion detection and intrusion prevention systems h. securing mail clients i. administering the mail server in a secure manner As suggested by its 2007 publication date, SP 800-45 does not reflect the most recent developments in email security, especially the more recent IETF RFCs (e.g., S/MIME Certificate Association (SMIMEA) 28 and TLS Certificate Association (TLSA) 29), but the recommendations it makes are still germane. With respect to the Cybersecurity Framework’s Identify Function and its Categories and Subcategories, SP 800-45 recommends risk management activities, but does not go into detail that maps to Subcategory references. Under the Protect Function, Subcategory references PR.AC-1, PR.AC-4, PR.AC-5, PR.AT-1, PR.AT-2, PR.AT-5, PR.DS-2, PR.DS-6, PR.IP-2, PR.IP-4, and PR.PT-1 are addressed by the guideline. Under the Detect Function, Subcategory references DE.DP-1 and DE.DP-4 are addressed by the guideline. In the Detect Function, Subcategory references DE.AE-2, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-8, DE.DP-1, and DE.DP-4 are addressed. Under the Respond Function, Subcategory references RS.RP-1, RS.CO-1, RS.CO-2, RS.AN-1, and RS.IM-1 are addressed by the guideline. Under the Recover Function, Subcategory reference RC.RP-1 is addressed by the guideline. 4. Federal S/MIME V3 Client Profile, NIST SP 800-49, Chernick, November 2002. https://doi.org/10.6028/NIST.SP.800-49. SP 800-49 was developed to provide organizations with approaches to assure that S/MIME products can interoperate and meet the email security needs of federal agencies both with respect to security features and adequate cryptographic algorithms. This profile states requirements for implementing sets of cryptographic algorithm suites specified elsewhere by the standards development organizations. The profile specifies a set of email security features (e.g., encrypted email and signed receipts) that are mandatory for federal agencies. SP 800-49 28 See Using Secure DNS to Associate Certificates with Domain Names For S/MIME (draft ietf-dane-smime-14). 29 RFC 6698, The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 25 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. adds specificity to the S/MIME standards, while attempting to avoid violating those standards. As its 2002 publication date suggests, SP 800-49 is even more dated with respect to protocols than SP 800-45 (e.g., recommending the now deprecated Secure Hash Algorithm 1 (SHA-1) instead of SHA-2 for hashing, and the deprecated Triple Data Encryption Standard (DES) rather than the Advanced Encryption Standard (AES) for encryption). However, it too makes security recommendations that are still germane. The SP 800-49 requirements and recommendations fall into the Cybersecurity Framework Protect Function. It provides guidelines that address the Subcategory references PR.DS-2, PR.DS-6, and (less precisely) PR.PT-4. 5. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations; NIST SP 800-52 Rev. 1; Polk, McKay, Chokhani; April 2014. https://doi.org/10.6028/NIST.SP.800-52r1. TLS provides mechanisms to protect sensitive data during electronic dissemination across the Internet. SP 800-52 provides guidance in the selection and configuration of TLS protocol implementations, while making effective use of FIPS and NIST-recommended cryptographic algorithms. SP 800-52 requires that TLS 1.1 be configured with FIPS-based cipher suites as the minimum appropriate secure transport protocol and recommends that agencies develop migration plans to TLS 1.2 by January 1, 2015. This SP also identifies TLS extensions for which mandatory support must be provided and some other recommended extensions. Like SP 800- 49, the SP 800-52 requirements and recommendations fall into the Cybersecurity Framework Protect Function. The guideline addresses Subcategory references PR.DS-2, PR.DS-6, and (less precisely) PR.PT-4. 6. Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800- 53 Rev. 4, Joint Task Force Transformation Initiative, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4. SP 800-53 provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation from a diverse set of threats, including hostile cyberattacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure that are derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, that are tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 26 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy. SP 800-53 Rev. 4 addresses all Cybersecurity Framework Functions, Categories, and Subcategories. Only the RC.CO-1 (Reputation after an event is repaired) and RC.CO-2 (Recovery activities are communicated to internal stakeholders and executive and management teams) references under the Recover: Communications Category are not addressed by SP 800-53. 7. Recommendation for Key Management: Part 1 - General, NIST SP 800-57 Part Rev.4, Barker, January 2016; Part 2 - Best Practices for Key Management Organization, NIST SP 800-57 Part 2, Barker, Barker, Burr, Polk, and Smid, August 2005; and Part 3 - Application-Specific Key Management Guidance, NIST SP 800-57 Part 3 Rev. 1, Barker and Dang, January 2015. https://doi.org/10.6028/NIST.SP.800-57pt1r4, https://doi.org/10.6028/NIST.SP.800-57p2, https://doi.org/10.6028/NIST.SP.800-57pt3r1 NIST SP 800-57 provides cryptographic key management guidance. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies. Part 3 of this SP provides guidance when using the cryptographic features of current systems that may not exhibit all the properties recommended by Part 1 of the guideline. Part 3 includes applications-specific recommendations for, among other applications, the Public Key Infrastructure (PKI), IPsec, TLS, S/MIME, and DNSSEC. All of these recommendations apply directly to this project. SP 800-57 addresses all of the Cybersecurity Framework Functions except Detect. Audit is the primary mechanism relied on in SP 800-53 for detection purposes. The Categories and Subcategory references that are addressed by the guideline include Identify (ID.AM-2, ID.BE-3, ID.BE-4, ID.BE-5, ID.GV-1, ID.GV-4, ID.RA-4, and ID.RA-5), Protect (PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AT-2, PR.AT-3, PR.AT-4, PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-4, PR.DS-6, PR.IP-2, PR.IP3, PR.IP-4, PR.IP-5, PR.IP-6, PR.IP-9, PR.PT-1, PR.PT-2, PR.PT-3, and PR.PT-4); Respond (RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3, RS.AN-2, and RS.MI-2); and Recover (RC.RP-1). 8. Secure Domain Name System (DNS) Deployment Guide, NIST SP 800-81-2, Chandramouli and Rose, September 2013. https://doi.org/10.6028/NIST.SP.800-81-2. The DNS is a distributed database that enables access to Internet resources via user-friendly domain names, rather than IP addresses, by translating domain names to IP addresses and back. The DNS infrastructure is made up of computing and communication entities called name servers, each of which contains information about a small portion of the domain name space. The name data provided by DNS is intended to be available to any computer located anywhere NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 27 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. in the Internet. SP 800-81-2 provides deployment guidelines for securing DNS within an enterprise. The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of name information and maintain the integrity of name information in transit. This document provides extensive guidance on maintaining data integrity and performing source authentication. This document presents guidelines for configuring DNS deployments to prevent many redirection attacks that exploit vulnerabilities in various DNS components. The Categories and Subcategory references that are addressed are limited to Identify (ID.AM-2 and ID.RA-6), Protect (PR.AC-1, PR.AC-3, PR.AC-5, PR.AT-2, PR.DS-2, PR.DS-5, PR.DS-6, PR.IP-3, PR.IP-4, PR.IP-6, and PR.IP-9), and Detect (DE.CM-1 and DE.CM-7). 9. A Framework for Designing Cryptographic Key Management Systems; NIST SP 800-130; Barker, Branstad, Smid, Chokhani; August 2013. https://doi.org/10.6028/NIST.SP.800-130. SP 800-130’s framework for designing Cryptographic Key Management Systems (CKMS) contains topics that should be considered by a CKMS designer when developing a CKMS design specification. For each topic, there are one or more documentation requirements that need to be addressed by the design specification. Thus, any CKMS that addresses each of these requirements would have a design specification that is compliant with this framework. A CKMS will be a part of a larger information system that executes processing applications. While the CKMS supports these applications by providing cryptographic key management services, the particular applications or particular classes of applications are beyond the scope of this framework. SP 800-130 addresses all the Cybersecurity Framework Functions. The Category and Subcategory references that are addressed include Identify (ID.BE-4, ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4, ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-5, and RM-1); Protect (PR.AC-1, PR.AC-2, PR.AC-4, PR.AC-5, PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5, PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-6, PR.DS-7, PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-6, PR.IP-9, PR.MA-1, PR.PT-1, PR.PT-2, PR.PT-3, and PR.PT-4); Detect (DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8,DE.DP-1, DE.DP-2, DE.DP-3, and DE.DP-5); Respond (RS.RP-1, RS.CO-1, RS.CO-2, RS.AN-2, RS.MI-1, and RS.MI-2); and Recover (RC.RP-1). 10. A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS); NIST SP 800-152; Barker, Branstad, Smid; October 2015. https://doi.org/10.6028/NIST.SP.800-152. SP 800-152 covers major aspects of managing the cryptographic keys that protect federal information. Associated with each key is specific information (e.g., the owner identifier, its length, and acceptable uses) called metadata. The computers, software, modules, communications, and roles assumed by one or more authorized individuals when managing and using cryptographic key management services are collectively called a Cryptographic Key NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 28 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Management System (CKMS). The Profile for U. S. Federal Cryptographic Key Management Systems (FCKMSs) has been prepared to assist CKMS designers and implementers in selecting the features to be provided in their “products,” and to assist federal organizations and their contractors when procuring, installing, configuring, operating, and using FCKMSs. SP 800-130 addresses all the Cybersecurity Framework Functions. The Categories and Subcategory references that are addressed include Identify (ID.AM-3, ID.AM-5, ID.BE-4, ID.BE-5, ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4, ID.RA-1, ID.RA-3, ID.RA-5, ID.RA-6, RM-1, and RM-2); Protect (PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5, PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-4, PR.DS-6, PR.DS-7, PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-5, PR.IP-6, PR.IP-7, PR.IP-8, PR.IP-9, PR.IP-12, PR.MA-1, PR.PT-1, PR.PT-2, PR.PT-3, and PR.PT-4); Detect (DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, DE.DP-1, DE.DP-2, DE.DP-3, and DE.DP-5); Respond (RS.RP-1, RS.CO-1, RS.CO-2, RS.AN-2, RS.MI-1, RS.MI-2, RS.MI-3, and RS.IM-2); and Recover (RC.RP-1 and RC.IM-2). 11. Trustworthy Email; NIST SP 800-177; Chandramouli, Garfinkel, Nightingale, and Rose; September 2016. https://doi.org/10.6028/NIST.SP.800-177 NIST SP 800-177 serves as a complimentary document to SP 800-45. SP 800-177 addresses email protocol security and provides descriptions, guidelines and recommendations for deploying new email security protocols such as SMTP over TLS, email supported by DANE, and other non-cryptographic authentication (e.g. Sender Policy Framework). Discussions of SMTP over TLS and S/MIME relate directly to the work on the project. With respect to the Cybersecurity Framework’s Identify Function and its Subcategories, SP 800- 177 recommends risk management activities, but does not go into detail that maps to subcategory references. Under the Protect Function, Subcategory references PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AT-1, PR.AT-2, PR.AT-5, PR.DS-2, PR.DS-6, PR.IP-2, PR.IP-4, and PR.PT-1 are addressed by the guideline. Under the Detect Function, Subcategory references DE.AE-2, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-8, DE.DP-1, and DE.DP-4 are addressed by the guideline. Under the Respond Function, Subcategory references RS.RP-1, RS.CO-1, RS.CO-2, RS.AN-1, and RS.IM-1 are addressed by the guideline. Under the Recover Function, Subcategory reference RC.RP-1 is addressed by the guideline. 3.4.6 Other Security References Applied in the Design and Development of the Project The following references provided additional security and protocol standards and guidelines that were applied during design and development of the project. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 29 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 1. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST SP 800-160, November 2016. https://doi.org/10.6028/NIST.SP.800-160. NIST SP 800-160 defines systems security engineering processes that are tightly coupled to and fully integrated into well-established, international standards-based systems and software engineering processes. The project supports the federal cyber security strategy of “Build It Right, Continuously Monitor” and consisted of a four-phase development approach that culminated in the publication of this final systems security engineering guideline. The four phases included: • Phase 1: Development of the systems security engineering technical processes based on the technical systems and software engineering processes defined in Internet Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) 15288:2008; • Phase 2: Development of the remaining supporting appendices: Information Security Risk Management (including the integration of the RMF, security controls, and other security- and risk-related concepts into the systems security engineering processes), Use Case Scenarios, Roles and Responsibilities, System Resiliency, Security and Trustworthiness, Acquisition Considerations, and the Department of Defense Systems Engineering Process; • Phase 3: Development of the systems security engineering nontechnical processes based on the nontechnical systems and software engineering processes (i.e., Agreement, Organizational Project-Enabling, and Project) defined in ISO/IEC/IEEE 15288:2008; and • Phase 4: Alignment of the technical and nontechnical processes based on the updated systems and software engineering processes defined in ISO/IEC/IEEE DIS 15288:201x (E). The full integration of the systems security engineering discipline into the systems and software engineering discipline involves fundamental changes in the traditional ways of doing business within organizations—breaking down institutional barriers that, over time, have isolated security activities from the mainstream organizational management and technical processes, including, for example, the system development life cycle, acquisition/procurement, and enterprise architecture. The integration of these interdisciplinary activities requires the strong support of senior leaders and executives, and increased levels of communication among all stakeholders who have an interest in, or are affected by, the systems being developed or enhanced. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 30 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 2. Internet X.509 Public Key Infrastructure Certificate and CRL Profile; IETF RFC 2459; Housley, Ford, Polk, Solo; January 1999. https://datatracker.ietf.org/doc/rfc2459. RFC 2459 is one part of a family of standards for the X.509 PKI for the Internet, but the RFC is a standalone document; implementations of this standard proceed independent from the other parts. The RFC profiles the format and semantics of public key certificates and certificate revocation lists for the Internet. Procedures are described for the processing of certification paths in the Internet environment. Encoding rules are provided for popular cryptographic algorithms. Finally, Abstract Syntax Notation One (ASN.1) modules are provided in the appendices for all data structures defined or referenced. 3. Threat Analysis of the Domain Name System (DNS), IETF RFC 3833, Atkins and Austein, August 2004. https://datatracker.ietf.org/doc/rfc3833. RFC 3833 attempts to document some of the known threats to the DNS, and, in doing so, measure the extent to which DNSSEC is a useful tool in defending against these threats. 4. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; Proposed Standard; IETF RFC 5280; Cooper, Santesson, Farrell, Boeyen, Housley, Polk; May 2008. https://datatracker.ietf.org/doc/rfc5280. RFC 5280 profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet. The RFC provides an overview and model of the specified approach, describes the X.509 v3 certificate format in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is also specified, the X.509 v2 CRL format is described along with standard and Internet-specific extensions, an algorithm for X.509 certification path validation is described, and an ASN.1 module and examples are provided. 5. Simple Mail Transfer Protocol, IETF RFC 5321, Draft Standard, Kleinstein, October 2008. https://datatracker.ietf.org/doc/rfc5321. RFC 5321 is a specification of the basic protocol for Internet email transport. It covers the SMTP extension mechanisms and best practices for the contemporary Internet, but does not provide details about particular extensions.