Appendix D. IT Security Capability Definitions

NIST Framework Function	Capability	Definition
Identify	Application Management	The practice of managing endpoint applications, including operating systems, to insure that deprecated, security vulnerable applications are known to all, they are detected if used, their execution is controlled/blocked by application whitelists, and ultimately, that common approved applications are resilient even to unknown exploits via advanced execution control techniques that interdict the cybersecurity attack chain.
Identify	Asset Management	The practice of tracking all known hardware assets of the enterprise, including manual, partially automated, fully automated, and continuous updates to the hardware attributable or connected to enterprise networks. Asset information includes machine type models, basic configurations, serial numbers, asset tags, user assignment and so forth. Full configuration control and update is part of configuration management.
Identify	Mobile Endpoint Management	The practice of managing mobile endpoints – from user provisioning, usage restrictions, geotagged security, applications allowed (mobile app management) – from cradle to grave. From a security standpoint, also maintaining standards for connection/communication with the enterprise network (e.g., e-mail, virtual desktop, other types of direct connection to enterprise systems).
Identify	Software Refreshment	The practice of managing enterprise systems, including operating systems and components of custom-developed systems, to insure that deprecated, security vulnerable software are known to all, they are detected if used, their execution is controlled/blocked by application whitelists, and ultimately, that common approved applications are resilient even to unknown exploits via advanced execution control techniques that interdict the cybersecurity attack chain.
Identify	Federal Government Outreach	Public-private partnerships, to include partners outside the Federal Government such as the Defense Industrial Base, owners of critical infrastructure, universities and other academia, and state and local governments. This also includes identifying, assessing, and mitigating cyber risks to mission essential functions in the nation's key critical infrastructures (previously "Public-Private Partnerships: Risk Management").
Identify	International Diplomacy	To include the costs of working with other governments to further cooperation on cybersecurity, including the development of cooperative activities for improving cybersecurity, international cooperation to investigate cyber incidents, safeguards for privacy, commercial transactions, and agreements on cybersecurity activities.
Identify	Standards Development and Propagation	Cybersecurity is becoming more standards-based to further improve automation, interoperability, and efficiency. NIST has the lead to develop standards, coordinate, and support Agencies.
Identify	Advisory Committee Activities	Statutorily defined advisory councils such as the Critical Infrastructure Partnership Advisory Council and the National Security Telecommunications Advisory Committee.
Identify	Other Identify Capabilities	To include other cybersecurity costs associated with the Identify function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Identify Capabilities should not

NIST Framework Function	Capability	Definition
		exceed $10 million. If Agency spending for Other Identify Capabilities exceeds $10 million, Agencies should break the Investment into smaller individual components and describe them in greater detail.
Detect	Audit and Event Logging	The practice of maintaining full logs of all system activity, both internal and weblogs of externally-focused applications. System logs should be maintained and monitored by the developer teams and the associated systems security office. Beginning with web-facing systems, logs should be aggregated and ultimately fed into an enterprise security warehouse to assist in understanding security events that may have impacted the system in question.
Detect	Command & Control (CNC) Interdiction	The practice of blocking outbound traffic that is initiated by external, unapproved command & control type requests by an external CNC host. Can be as simple as URL blacklisting to more sophisticated DNS sinkholing and advanced CNC interdiction techniques.
Detect	Intrusion Detection	The practice of monitoring system activity through examining system traffic – both inbound and outbound – to match known intrusion patterns with the traffic, based on threat signatures provided by a vendor or developed internally.
Detect	Malware Analysis	The practice of analyzing a particular instance of malware to understand its behavior and what it is attempting to accomplish. This can be done through direct code analysis, out of band testing, creating a virtual sandbox for testing, or in-line, automated sandboxing, which may divert the malware, test it, then strip it out of network traffic or e-mail.
Detect	Malware Remediation	The practice of remediating the impacts of a particular instance of malware to return the system, application or e-mail to normal, non-threatening behavior. This can be done through restoration points; malware quarantine & deletion out of band; out of band payload removal, or in-line, automated content detonation/payload removal; and advanced execution control, which blocks payload execution at the process level in common applications.
Detect	Traffic Scanning	The practice of scanning all network traffic to identify, understand, and visualize traffic flow; capture, examine, and potentially block individual packets; and perform deep inspection – including encrypted traffic – to identify threats.
Detect	Anti-Phishing	The practice of implementing technologies and processes and that reduce the risk of malware introduced through e-mail and social engineering. This includes anti-phishing and -spam filters; analyzing incoming e-mail traffic using sender authentication, reputation filters, embedded content detection, and suspicious attachments; and utilizing end user authentication protocols on outgoing e-mail traffic to allow recipients to verify the originator.
Detect	Data Loss Prevention (DLP)	DLP is the practice of discovering sensitive content and blocking its exfiltration from the control of the enterprise. DLP systems are principally concerned with the data exiting a perimeter gateway, including emails, instant messages and Web 2.0 applications; however, this can be extended to copying of sensitive data to other media such as thumb drive, inappropriate collection and storage on a user endpoint, or printing of sensitive data.
Detect	Intrusion Prevention	The practice of intrusion prevention involves blocking and reporting suspicious activity on the enterprise perimeter or network. These can be security threats or policy violations. Intrusion prevention can include

NIST Framework Function	Capability	Definition
		dropping of malicious packets, blocking/filtering a specific URL, and so forth.
Detect	Threat Intelligence & Information Sharing	The practice of analyzing malware and determining its source, developing threat signatures, and sharing of the information within the security enterprise as well as to the larger security community.
Detect	Other Detect Capabilities	To include other cybersecurity costs associated with the Detect function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Detect Capabilities should not exceed $10 million. If Agency spending for Other Detect Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.
Protect	Configuration Management	Configuration management is the discipline and processes that to keep track of how hardware, operating systems, software versions and updates that are installed are deployed as part of the enterprise computing infrastructure. From a security standpoint, using unauthorized configurations is a negative and changes to configurations may be indicators of compromise that should be blocked from access until remedied.
Protect	Data Safeguarding – Data At Rest	Safeguarding data at rest involves strong data encryption. This begins with individual encrypted files, progressing to device encryption, data set encryption, etc. Ultimately, it can include data destruction to prevent compromise, including such concepts as remote data wiping and ephemeral data.
Protect	Data Safeguarding – Data in Motion	Safeguarding data in motion requires encryption as well, starting with methods of encrypted file transfer, encrypted emails, and progressing through transport layer security/SSL to virtual private networks to highly secure individual data networks.
Protect	Data Visibility	The practice of preventing casual insider threats to data, including timed lock screens on endpoints; data masking/obfuscation for high security data being accessed by developers/non-privileged users; surveying privileged user activity, including keystroke, videotaping, etc.; network detection of anomalous end-user behavior; and creating an end user culture of security which recognizes and reports potential insider threats.
Protect	Internet Access Management	The practice of managing how the enterprise connects to the public Internet, including ad hoc connections (dial-up, private lines, etc.), though self-managing of central gateways, to using the federal TIC and Managed Trusted Internet Protocol Service (MTIPS) services.
Protect	Vulnerability Analysis	Assessing the vulnerability of an enterprise by multiple means of vulnerability scanning and penetration testing, including automated PenTesting, formal Red Team Exercise, and continuous Red Team hacking to identify remaining vulnerabilities.
Protect	Vulnerability Management	Assessing the vulnerability of a particular system by a variety of techniques, including review of the system logs for exploitable errors, formal system vulnerability testing, automated testing and scanning, and ultimately leading to a security-by-design development approach.
Protect	Security Training	The practice of providing or otherwise ensuring users complete appropriate Cybersecurity Awareness and Training (CSAT). This includes conducting phishing exercises and role-specific training for users with significant security capabilities.

NIST Framework Function	Capability	Definition
Protect	Credentialing	Credentialing is a system by which identification cards or other tokens are used to authenticate a person and transmit skills, qualifications, and other attributes associated with that identity. This includes requiring authentication to access data/data systems; utilizing a physical token (e.g., ID badge) that reflects a particular level of assurance (LOA) required for access to a physical or logical enterprise enclave; verifying and maintaining the verification of a particular end-user's identity; federating the identities/access/authorities granted; and confirming the identity of a potential user before being allowed access to the physical or logical enclaves of the enterprise.
Protect	Authorization and Least Privilege	Least privilege is the principle that only the minimum necessary rights should be assigned to a subject and should be in effect for the shortest duration necessary. This includes managing the particular usage rights an authorized user has on a device or system; utilizing mechanisms by which a previously authenticated users are allowed to perform actions such as using a particular system within the enterprise; and ensuring authorization after access involves the user roles assigned and the access privileges this extends to data systems.
Protect	Cloud Services	The practice of acquiring cloud services and applications and ensuring they meet adequate security expectations. This includes assessing potential cloud services for alignment with established FedRAMP security baselines; acquiring tools to enhance the security of cloud-based applications; and the granting of ATOs to cloud service providers.
Protect	Counterintelligence	Information gathered and activities conducted to protect against cyber espionage, other intelligence activities, or sabotage conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities.
Protect	Research & Development	R&D related to cybersecurity and information assurance to protect computer-based systems from actions that compromise or threaten to compromise the authentication, availability, integrity, or confidentiality of these systems and/or the information they contain.
Protect	Other Protect Capabilities	To include other cybersecurity costs associated with the Protect function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Protect Capabilities should not exceed $10 million. If Agency spending for Other Protect Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.
Respond	Incident Management & Response	Case management – recording, ticketing, tracking, reporting, resolution – of a security incident; Security Operations Center (SOC) operators.
Respond	Federal Incident Response Centers	Government focal points for dealing with computer-related incidents affecting federal civilian Agencies. The centers provide a means for federal civilian Agencies to work together to handle security incidents, share related information, and solve common security problems.
Respond	Prosecution and Investigation of Cyber Intrusions	This includes the process of gathering evidence, attributing criminal acts to specific individuals, and pursuing criminal charges or civil actions against cyber perpetrators. This also includes actions associated with the investigation or prosecution of a criminal violation taken to reduce the extent or consequence of an adverse event affecting information systems, the information residing therein, or supported infrastructure (Previously Law Enforcement: Incident Response).

NIST Framework Function	Capability	Definition
Respond	Other Respond Capabilities	To include other cybersecurity costs associated with the Respond function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Respond Capabilities should not exceed $10 million. If Agency spending for Other Respond Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.
Recover	Disaster Recovery	Disaster recovery is the practice of returning a system or systems to operating capability by using back-up and restore techniques, duplicate "continuity of operations (COOP) sites", cloud-based restoration, or full cloud-based COOP operations.
Recover	Incident Notification	The practice of providing public/internal notifications to potentially impacted persons following cybersecurity incidents involving the possible loss of personally identifiable information (PII) and offering remediation for those adversely affected. This includes assessing potential impact to the public or internal populations; issuing public/internal notifications following an incident; tracking the issuance of notifications; and the acquisition and use of credit monitoring and credit repair services.
Recover	Other Recover Capabilities	To include other cybersecurity costs associated with the Recover function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Recover Capabilities should not exceed $10 million. If Agency spending for Other Recover Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.