State of California

Office of Information Security

Foundational Framework

SIMM 5300-B

October 2017

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	November 2017	Office of Information Security	New

TABLE OF CONTENTS

I. INTRODUCTION

The Department of Technology, Office of Information Security has established this foundational framework comprised of 30 priority security objectives to assist state entities with prioritization of their information security efforts. The foundational framework is considered a starting point and will be used to consistently measure and mature state entity security compliance moving forward.

As state entities achieve compliance with foundational framework objectives they will continue to address other applicable control areas to sufficiently protect information assets and address organizational risk.

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
APPLICATION SECURITY	**Establish security controls for the development, acquisition, and use of software applications that are commensurate with the defined security risk for use and operations of those applications.**	**Application Inventory Management**: Develop a formal, comprehensive software application inventory management process that includes regular and periodic reviews, management and stakeholder input and approval, integration with enterprise asset management processes	**Identify**	Formally defined, documented, and centrally managed software inventory management process, mandated by policy with senior management oversight, with regular and periodic review and update of inventory contents.	**5305.5** Information Asset Management **5315.3** Information Asset Documentation **5315.7** Software Usage Restrictions	**Configuration Management:** **CM-8** INFORMATION SYSTEM COMPONENT INVENTORY **PM-5** INFORMATION ASSET INVENTORY
				Use of automated tools for software discovery and inventory content maintenance with owner and stakeholder input.		
				Inventory contents include associated software characteristics include owners, assurance and protection requirements, sensitive data stored or processed, infrastructure requirements, aging and skill set requirements.		
				Approach and applicability of the enterprise software inventory and contents is enhanced and enforced through a regular and periodic program of review, audit, and update.		
		Application Assurance Level Definition: Define application assurance levels based on criticality to business mission and sensitivity of data, as well as operational threat environment	**Identify**	Application assurance levels have been formally defined, documented and governed through enterprise application development policy with senior management oversight.	**5315** Information Security Integration **5315.2** SDLC **5315.1** System and Services Acquisition	**System and Services Acquisition:** **SA-8** SECURITY ENGINEERING PRINCIPLES **SA-11** DEVELOPER SECURITY TESTING AND EVALUATION
				All applications are regularly and periodically assessed.		
				Threats, vulnerabilities, and consequences are used to identify the security requirements of the application in terms of business requirements.		
				Assurance ratings are maintained as part of application inventory management process, and used to define appropriate secure coding and testing methodologies.		
				Assurance definitions and assignments are enhanced and enforced through a regular and periodic program of review, audit, and update.		
		Secure Code Practices: Establish and deploy software development and programming methods, techniques and standards (secure coding practices) used specifically for implementing software in a way that prevents, avoids, or does not create security vulnerability in the resulting application	**Protect**	Secure coding practices (software development and programming methods, techniques and standards) are formally defined, documented and governed through enterprise application development policy with senior management oversight.	**5315** SDLC	**System and Services Acquisition:** **SA-17** DEVELOPER SECURITY ARCHITECTURE AND DESIGN **CM-7** LEAST FUNCTIONALITY **SI-10** INFORMATION INPUT VALIDATION
				Practices are defined, documented, integrated, and enforced across all system development environments.		
				App developers are regularly and periodically trained and secure coding practices for applicable system development environments.		
				Practices are enhanced and enforced through a regular and periodic program of review, audit, and update.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
CONTINGENCY PLANNING	**Deploy controls to prevent unauthorized or unacceptable loss of customer, critical, and sensitive information. In keeping with a systematic and comprehensive security program, deploy controls to protect information availability.**	**Business Impact Assessment**: Develop and vet an enterprise Business Impact Analysis (BIA) with realistic Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) commensurate with assurance-level of each application and aligned with service recovery objectives established in enterprise Business Continuity Plan (BCP)	**Recover**	Enterprise Business Impact Analysis (BIA) is conducted regularly and periodically resulting in realistic Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems and supporting IT infrastructure.	**5325** Business Continuity with Technology Recovery **5325.1** Technology Recovery Plan **5325.4** Alternate Storage and Processing Site **5325.5** Telecommunications Services	**Contingency Planning:** **CP-2** CONTINGENCY PLAN **CP-4** CONTINGENCY PLAN TESTING **CP-6** ALTERNATE STORAGE SITE **CP-7** ALTERNATE PROCESSING SITE
				Recovery objectives are commensurate with assigned assurance-level of each application and aligned with service recovery objectives established in the enterprise Business Continuity Plan (BCP).		
				Service recovery objectives are reviewed and approved by key business process stakeholders.		
				BIA is reviewed and updated at least annually with a complete refresh at least every three years.		
				Disaster recovery testing results are used as feedback to periodically enhance BIA-based recovery objectives between BIA refresh cycles.		
		Comprehensive DRP Testing: Existing disaster recovery processes to include periodic live testing of recovery capabilities and incorporating feedback to refine the processes	**Recover**	Disaster Recovery (DR)/Business Continuity (BC) testing is conducted as part of a formal, documented plan integrated with the regular and periodic review of the DR/BC plans.	**5325.1** Technology Recovery Plan **5325.3** Technology Recovery Testing **5325.6** Information System Backups	**Contingency Planning:** **CP-2** CONTINGENCY PLAN **CP-3** CONTINGENCY TRAINING **CP-4** CONTINGENCY PLAN TESTING **CP-9** INFORMATION SYSTEM BACKUP
				Testing is structured as a tiered testing program that includes table-top scenario-based and live partial (function, infrastructure, system or application-specific) recovery testing, as well as live, full failover and recovery testing for all systems supporting critical business processes.		
				Test results are used as feedback to the plan review process and incorporated as refinements to the plan.		
				Testing occurs at least annually.		
				Full, live testing occurs at least every three years.		

SIMM 5300-B FOUNDATIONAL FRAMEWORK

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
CHANGE AND CONFIGURATION MANAGEMENT	**Establish change and configuration management controls that include a workflow model with documentation, attribution, approval processes, testing, and execution of the change. Additionally, establish controls to protect the integrity and confidentiality of the change management process commensurate with level of criticality of the resources being changed.**	**Comprehensive Enterprise Change Management Process, Workflow, and Database**: Establish organization-wide change management (CM) process and standards applicable to all IT and information (hardware, software, infrastructure, and data); support change management process with single automated workflow tool and central CM data repository	**Identify**	Practices are formally defined and governed by enterprise policy with senior management oversight.	**5315.5** Configuration Management **5315** Information Security Integration	**Configuration Management:** **CM-3** CONFIGURATION CHANGE CONTROL **CM-4** SECURITY IMPACT ANALYSIS **CM-5** ACCESS RESTRICTIONS FOR CHANGE
				Enterprise policy is comprehensively applied across the enterprise; mandates the maintenance of an enterprise change management processes; and defines the assets to be managed via the process; outlines specific management and administration responsibilities including change advisory board (CAB) and formal security change impact evaluations.		
				Implementation includes the use of automation for workflow, cataloging, tracking, and reporting.		
				Monitoring and reporting processes are defined and established to ensure policy adherence.		
				Integrated with enterprise configuration and asset management processes.		
				Approach and applicability of the change management policy is enhanced and enforced through a regular and periodic program of review, audit, and approach update.		
		Embed Formal Security Evaluations in Enterprise CM Process: Integrate formal security impact evaluation and approval in enterprise risk management processes and panels	**Detect**	Practices are formally defined and governed by enterprise policy with senior management oversight.		**Configuration Management:** **CM-4** SECURITY IMPACT ANALYSIS
				Enterprise policy is comprehensively applied across the enterprise; mandates the maintenance of an enterprise change management process that includes formal security change impact evaluations to qualify the level of alteration to the enterprise security posture resulting from the proposed change; defines the threshold criteria for identifying types of changes subject to security impact evaluations; outlines specific management and administration responsibilities including actions and authority of change advisory board (CAB) to stop, suspend, or approve changes based on results of security impact evaluation.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
DATA SECURITY	**Deploy governance processes and protection controls to prevent unauthorized or inappropriate access to or disclosure of private or sensitive information. In keeping with a systematic and comprehensive security program, deploy controls to protect information confidentiality in addition to controls for other major security objectives as they relate to comprehensive data and information protection.**	**Data Classification Policy and Enforcement**: Establish enterprise policy and practices for data classification that includes identification and definition of data and information types used, processed, and stored throughout the enterprise in alignment with business processes	**Identify**	Business data use cases and practices are formally defined and governed by enterprise policy with senior management oversight.	**5305.5** Information Asset Management **5310.1** State Entity Privacy Statement And Notice On Collection **5310.2** Limiting Collection **5310.3** Limiting Use And Disclosure **5310.4** Individual Access to Personnel Information **5310.5** Information Integrity **5310.6** Data Retention and Destruction **5310.7** Security Safeguards **5320** Training and Awareness for Information Security and Privacy **5365.2** Media Protection **5365.3** Media Disposal	**Awareness and Training Risk Assessment:** **RA-2** SECURITY CATEGORIZATION **System and Communications Protection:** **SC-8** TRANSMISSION CONFIDENTIALITY AND INTEGRITY **SC-13** CRYPTOGRAPHIC PROTECTION **SC-28** PROTECTION OF INFORMATION AT REST
				Enterprise policy defines practices for data classification that includes identification and definition of data and information types used, processed, and stored throughout the enterprise in alignment with business processes.		
				Authorized use case guidelines are provided for data-at-rest, in-motion, and in-use, as well as required standards for protection per use case.		
				Use case requirements include data exchange, retention, and destruction, as well as hardcopy and mobile media applicability.		
				Training on appropriate use is included in regular and periodic security awareness program.		
				Monitoring and reporting processes are defined and established to ensure policy adherence.		
				Approach and applicability of the enterprise data classification policy is enhanced and enforced through a regular and periodic program of review, audit, and approach update.		
		Data Privacy Program and Enforcement: Establish an enterprise policy and direct the development and maintenance of an organizational Privacy Program that defines the overall Privacy Program as it explicitly describes the applicability of privacy policy to enterprise business processes and ensures the compliance with the California Information Practices Act.	**Protect**	Enterprise privacy policy is defined with senior management accountability. Appoints a Chief Privacy Officer (CPO) or Privacy Coordinator (PC) responsible for the development, implementation, maintenance of a privacy program to protect individual privacy and to ensure the compliance with applicable laws and regulations regarding the collection, use, maintenance, sharing and disposal of personally information by programs and information systems.	**5305.2** Policy, Procedure and Standards Management **5305.6** Risk Management **5305.7** Risk Assessment **5310.1** State Entity Privacy Statement and Notice on Collection **5310.2** Limiting Collection **5310.3** Limiting Use and Disclosure **5310.4** Individual Access **5310.5** Information Integrity **5310.6** Data Retention and Destruction **5315.3** Information Asset Documentation **5330.1** Security Assessments	**Accountability, Audit, and Risk Management:** **AR-1** GOVERNANCE AND PRIVACY PROGRAM **AR-2** PRIVACY IMPACT AND ASSESSMENT **AR-3** PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS **AR-4** PRIVACY MONITORING AND AUDITING **AR-6** PRIVACY REPORTING **AR-7** PRIVACY ENHANCED SYSTEM DESIGN AND DEVELOPMENT **AR-8** ACCOUNTING OF DISCLOSURES **Risk Assessment:** **RA-1** RISK ASSESSMENT POLICY AND PROCEDURES **Program Management:** **PM-9** RISK MANAGEMENT STRATEGY **Authority and Purpose:** **AP-1** AUTHORITY TO COLLECT **AP-2** PURPOSE SPECIFICATION **Data Minimization and Retention:** **DI-1** MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION **Individual Participation and Redress:** **IP-1** CONSENT **Transparency:** **TR-1** PRIVACY NOTICE
				Policy is defined to support achievement of privacy objectives commensurate with business objectives.		
				Policies are regularly and periodically reviewed and updated for alignment with current prevailing industry practices and applicable threats.		
				Policies and any updates are regularly and periodically communicated to personnel with respect to applicability and enforcement.		
				Policy is supported by comprehensive, set of defined policy implementation standards and guidelines, as well as requirements for minimum baseline policy enforcement across all aspects of the architecture and business processes.		
				Privacy policy definition, applicability, and enforcement is enhanced and validated through a program of regular and periodic review, maintenance, update, monitoring and audit.		
				All public websites contain a Privacy Policy Statement. All online and hard copy forms that collect personal information contain a Notice on Collection.		
				Comprehensive privacy risk assessment strategy is formally defined and governed by the enterprise privacy policy with senior management oversight.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
DATA SECURITY, (CONT'D).			**Protect**	Policy identifies privacy-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Regular and periodic assessment of privacy-related risk and formal acceptance of residual risk by accountable organization management for programs, systems and technologies and including existing and new through informal and formal project management processes include Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA).		
				The assessment process is based on an industry-accepted leading practice privacy framework and includes criteria for qualifying risk commensurate with the business mission of the organization.		
				Process addresses residual risk in all aspects of the enterprise including telecommunications perimeter, major systems and applications, infrastructure, resources and data, governance, and procurement/acquisition.		
				The process is enforced through a program of regular and periodic monitoring and testing to validate assessment findings, with resulting metrics used to provide input to residual risk acceptance process.		
				Privacy program is periodically supplemented by privacy assessments conducted by independent third-parties.		
				Privacy assessment results are provided as input into overall enterprise risk and compliance management processes.		
				Privacy assessment processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		
		Protecting Confidential and Sensitive Data: Employ encryption technology to protect sensitive data-at-rest, in accordance with the enterprise data classification policy, in all enterprise and organization-specific structured data repositories that contain sensitive information including databases and enterprise content management systems	**Protect**	Data-at-rest protection practices are defined and governed in accordance with the enterprise information classification policy requirements for sensitive data.	**5310.7** Security Safeguards **5350.1** Encryption **5365.2** Media Protection **5350** Operational Security	**Media Protection:** **MP-5** MEDIA TRANSPORT **System and Communications Protection:** **SC-12** CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT **SC-17** PUBLIC KEY INFRASTRUCTURE CERTIFICATES **SC-28** PROTECTION OF INFORMATION AT REST **SC-8** TRANSMISSION CONFIDENTIALITY AND INTEGRITY **SC-13** CRYPTOGRAPHIC PROTECTION
				Appropriate, current-state technological protection, such as encryption, masking and obfuscation, or tokenization, are employed on all enterprise and organization-specific electronic media and devices with the capability to store information.		
				Encryption strength (key and algorithm) is commensurate with assurance-level requirements of the devices and media, as well as use cases in which the devices and media are used.		
				Encryption approach(es) are supplemented with sufficient encryption key management processes to ensure protected and managed data recovery for loss, mis-configuration, or forensic investigation.		
				Data-at-rest protection practices are enhanced and enforced through a regular and periodic program of review, audit, testing, and update.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
SECURITY GOVERNANCE	**Establish a high-level enterprise Security Governance process led by an information security officer (ISO) who is empowered to protect enterprise IT assets while removing the barriers to productivity through well-understood management processes and governance principles.**	**Awareness Training Program**: Establish a comprehensive enterprise security awareness and training policy with requirements for regular and periodic (annual) awareness training for all users of IT operated by or on behalf of the enterprise	**Respond**	Regular and periodic security awareness training is mandated by enterprise security policy with senior management oversight. Awareness training is mandatory for all enterprise personnel, as well as all vendors, suppliers, and providers which make use of or operate IT resources and information on behalf of the organization. Training compliance is formally tracked, managed, and reported, and enforced through suspension of access to IT assets required for job function. Training content includes awareness of security policy applicability and enforcement, applicable threats, and reporting. Training content is regularly and periodically updated to maintain currency with prevailing events. Training program is multi-faceted to include formal training, mass communications, and topic-specific messaging. Training program includes role-specific training for audiences from at least the general-user, technical, and management perspectives. Metrics exist to measure success of awareness program as it relates to improved security and decreased risk. Security awareness training program is enhanced through a program of regular and periodic review, maintenance, update, and audit.	**5305.4** Personnel Management **5320** Training And Awareness For Information Security And Privacy **5320.1** Security And Privacy Awareness **5320.2** Security And Privacy Training **5320.3** Security And Privacy Training Records **5320.4** Personnel Security	**Awareness and Training:** **AT-1** SECURITY AWARENESS POLICY AND PROCEDURES **AT-2** SECURITY AWARENESS TRAINING **AT-3** ROLE-BASED SECURITY TRAINING **AT-4** TRAINING RECORDS **Security Planning:** **PL-4** RULES OF BEHAVIOR
		Comprehensive Security Policy Structure: Formally establish and document a consolidated, comprehensive enterprise-specific security governance policy structure that includes policy, requirements, and supporting standards	**Protect**	Enterprise security policy is defined with senior management accountability. Policy is defined to support achievement of security objectives commensurate with business objectives. Policy is regularly and periodically reviewed and updated for alignment with current prevailing industry practices and applicable threats. Policy updates are regularly and periodically communicated to personnel with respect to applicability and enforcement. Policy is supported by comprehensive, set of defined policy implementation standards and guidelines, as well as requirements for minimum baseline policy enforcement across all aspects of the security architecture and all business processes.	**5305** Information Security Program **5305.2** Policy, Procedures and Standards Management	**Access Control:** **AC-1** ACCESS CONTROL POLICY AND PROCEDURES **Awareness and Training:** **AT-1** SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES **Audit and Accountability:** **AU-1** AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES **Security Assessment and Authorization:** **CA-1** SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES **Configuration Management:** **CM-1** CONFIGURATION MANAGEMENT POLICY AND PROCEDURES **Contingency Planning:** **CP-1** CONTINGENCY PLANNING POLICY AND PROCEDURES **Identification and Authentication:** **IA-1** IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES **Incident Response:** **IR-1** INCIDENT RESPONSE POLICY AND PROCEDURES **Maintenance:** **MA-1** SYSTEM MAINTENANCE POLICY AND PROCEDURES **Media Protection:** **MP-1** MEDIA PROTECTION POLICY AND PROCEDURES **Physical and Environmental Protection:** **PE-1** PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES **Planning:** **PL-1** SECURITY PLANNING POLICY AND PROCEDURES **Personnel Security:** **PS-1** PERSONNEL SECURITY POLICY AND PROCEDURES **Risk Assessment:** **RA-1** RISK ASSESSMENT POLICY AND PROCEDURES **System and Services Acquisition:** **SA-1** SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES **System and Communications Protection:** **SC-1** SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES **System and Information Integrity:** **SI-1** SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

SIMM 5300-B FOUNDATIONAL FRAMEWORK

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
SECURITY GOVERNANCE, (CONT'D).		**Security Management Plan**: Establish an enterprise policy and direct the development and maintenance of an organizational Security Management Plan (SMP) that defines the overall information protection program as it relates to security and privacy, and explicitly describes applicability of security and privacy policy to enterprise business processes	Protect	Comprehensive security and risk assessment strategy is formally defined and governed by the enterprise security management policy with senior management oversight.	**5305** Information Security Program **5305.1** Information Security Program Management **5305.2** Risk Management **5305.6** Risk Management **5305.7** Risk Assessment **5330.1** Security Assessments	**Security Assessment and Authorization:** **CA-7** CONTINUOUS MONITORING **Program Management:** **PM-1** INFORMATION SECURITY PROGRAM PLAN **Risk Assessment:** **RA-3** RISK ASSESSMENT **RA-1** RISK ASSESSMENT POLICY AND PROCEDURES
				Policy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Policy mandates process for residual security risk management that includes regular and periodic assessment of security-related risk and formal acceptance of residual risk by accountable organization management.		
				The assessment process is based on an industry-accepted leading practice security framework and includes criteria for qualifying risk commensurate with the business mission of the organization.		
				Process addresses residual risk in all aspects of the enterprise including telecommunications perimeter, major systems and applications, infrastructure, resources and data, governance, and procurement/acquisition.		
				The process is enforced through a program of regular and periodic monitoring and testing to validate assessment findings, with resulting metrics used to provide input to residual risk acceptance process.		
				Assessment program is periodically supplemented by assessments conducted by independent third-parties.		
				Assessment results are provided as input into overall enterprise risk and compliance management processes.		
				Security and risk assessment processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		
		Risk Acceptance: Formally establish an organization-specific policy and supporting process for residual security risk management that includes regular and periodic assessment of security-related risk and formal acceptance of residual risk by accountable organization management	Identify	Comprehensive security planning and system authorization strategy is formally defined and governed by the enterprise security management policy with senior management oversight.	**5305.6** Risk Management **5305.7** Risk Assessment **5315.9** Security Authorization	**Security Assessment and Authorization:** **CA-5** PLAN OF ACTION AND MILESTONES **CA-6** SECURITY AUTHORIZATION **Program Management:** **PM-4** PLAN OF ACTION AND MILESTONES PROCESS **PM-9** RISK MANAGEMENT STRATEGY **PM-10** SECURITY AUTHORIZATION PROCESS **Risk Assessment:** **RA-3** RISK ASSESSMENT
				Policy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Policy mandates the development and periodic maintenance of system-specific security plans, and requires senior management approval of the plans, as well as approval to operate the system or application in the risk environment documented in the plan.		
				Policy defines and identifies accountable management designated to formally accept residual risk per organization-specific criteria which includes overall responsibility for providing data and services to end-users, and the authority to provide and/or manage funding required to appropriately mitigate risks to an acceptable level.		
				Security plans align established security policy with applicable business-specific processes.		
				Security plans are established for all systems and applications identified as critical to the organization and successful execution of the business, and identify the approaches used to satisfy the confidentiality, availability, and integrity requirements of the systems and data processed, stored, or used by the system.		
				Security plans define the overall information protection approach applied to the system and application as it relates to security and privacy, including policies, processes, and controls.		
				Security planning and system authorization processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
SECURITY GOVERNANCE, (CONT'D).		**Procurement and Acquisition**: Establish and deploy contract terms and conditions as appropriate for enforcing enterprise security risk management policies and requirements in software, hardware, or services acquisition and procurement, including outsourced or other contracted efforts.	**Protect**	Procurement governance is formally established, including the identification of spend thresholds, and governed by enterprise policy.	**5230.4** Principles for IT Procurement **5305.8** Provisions for Agreements with State and Non-State Entities **5315** Information Security Integration **5330** Information Security Compliance **5315.1** System and Services Acquisition	**Access Control:** **AC-20** USE OF EXTERNAL INFORMATION SYSTEMS **Personnel Security:** **PS-7** THIRD-PARTY PERSONNEL SECURITY **System and Services Acquisition:** **SA-9** EXTERNAL INFORMATION SYSTEM SERVICES **SA-10** DEVELOPER CONFIGURATION MANAGEMENT **SA-4** ACQUISITION PROCESS **SA-4 (1)** Functional Properties of Security Controls
				Policy is aligned to the strategic business objectives and articulates the business value.		
				Procurement process workflow is documented to illustrate how stakeholders acquire IT systems/services.		
				Process includes incorporation of security-specific requirements commensurate with the type (hardware, software, services) and level of assurance of items being acquired.		
				Procurement decisions are documented for transparency, and the results are commensurate with established policy.		
				Procurement process is periodically assessed, improvement areas identified, and enhancements implemented.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
ENDPOINT SECURITY	**Deploy appropriate management and protection controls on endpoint platforms that will maintain stated security objectives for hosted data and applications under specific use cases, establish minimal controls for protecting systems, and enforce location-based policies with respect to applicable information, network, and application architectures. Choose a protection portfolio that includes preventative, detective, and responsive (react or adapt) technologies.**	**<u>Platform-Specific Build Standards and Procedures</u>**: Establish enterprise policy that directs the development and maintenance of organization-specific platform development / build standards, processes, and procedures	**Protect**	Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.	**5315.6** Activate Only Essential Functionality **5335.2** Auditable Events **5315.5** Configuration Management	**Configuration Management:** **CM-2** BASELINE CONFIGURATION **CM-2 (1)** Reviews and Updates **CM-3** CONFIGURATION CHANGE CONTROL
				Policy identifies specific management and administrative roles and responsibilities, including dependencies of vendors and contractors.		
				Practices include the application of security configuration hardening requirements that are based on industry-accepted standards for platform security configuration management.		
				Practices are applied comprehensively for all platform (hardware and operating system) types in the organization IT asset inventory.		
				Policy and standards align with and complement business-specific processes related to IT platform use.		
				Security hardening requirements are enforced through a program of regular and periodic review, maintenance, update, and audit.		
		<u>Platform-Specific Hardening Standards and Procedures</u>: Establish and document formal enterprise security policy and standards for platform configuration management including requirements for security configuration (hardening)	**Protect**	Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.	**5315.6** Activate Only Essential Functionality **5355** Endpoint Defense	**Configuration Management:** **CM-6** CONFIGURATION SETTINGS
				Policy identifies specific management and administrative roles and responsibilities, including dependencies of vendors and contractors.		
				Practices include the application of security configuration hardening requirements that are based on industry-accepted standards for platform security configuration management.		
				Practices are applied comprehensively for all platform (hardware and operating system) types in the organization IT asset inventory.		
				Policy and standards align with and complement business-specific processes related to IT platform use.		
				Security hardening requirements are enforced through a program of regular and periodic review, maintenance, update, and audit.		

SIMM 5300-B FOUNDATIONAL FRAMEWORK

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
IDENTITY AND ACCESS MANAGEMENT	**Establish an identity management service layer that provides consistent access control and policy enforcement; identity lifecycle and credential management; and identity data services for all subjects (users and services) and resources (systems, applications, data) in the environment.**	**Comprehensive Documented Enterprise Access Management and Provisioning Strategy**: Establish organization-specific access management processes that includes identity lifecycle management, consolidated and comprehensive use case provisioning and change management workflow, and centralized access authentication and authorization processes	**Protect**	Comprehensive identity and access management strategy is formally defined and governed by enterprise policy with senior management oversight. Enterprise policy is applied comprehensively for all business use cases. Policy identifies specific management and administrative roles and responsibilities, including applicability to vendors and contractors. Strategy is enforced through IAM-specific architecture and aligned with organization-specific business objectives and enterprise security objectives. Enterprise policy is enforced through use of provisioning processes to track, report, and validate individual user access rights and privileges. Policy is implemented through use of modern, enterprise-class automated provisioning and access management technology. Compliance and reporting requirements are enforced through the deployment of modern Governance-Risk-Compliance (GRC) technology integrated with provisioning processes. Strategy and policy, processes, and integrity of identity data is enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.	**5305.4** Personnel Management **5360** Identity and Access Management **5360.1** Remote Access **5360.2** Wireless Access **5365.1** Access Control for Output Devices	**Access Control:** **AC-1** ACCESS CONTROL POLICY AND PROCEDURES **AC-1 (1)** Automated Account Management **AC-1 (2)** Remove of Temporary/Emergency Accounts **AC-1 (3)** Disable Inactive Accounts **AC-1 (4)** Automated Audit Actions **AC-2** ACCOUNT MANAGEMENT **AC-3** ACCESS ENFORCEMENT **AC-5** SEPARATION OF DUTIES **AC-6** LEAST PRIVILEGE **Identification and Authentication:** **IA-1** IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES **IA-2** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) **IA-3** DEVICE IDENTIFICATION AND AUTHENTICATION **IA-4** IDENTIFIER MANAGEMENT **IA-5** AUTHENTICATOR MANAGEMENT **IA-8** IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) **Personnel Security:** **PS-3** PERSONNEL SCREENING **PS-5** PERSONNEL TRANSFER **PS-6** ACCESS AGREEMENTS
		Multi-Factor Authentication for Elevated Risk Use Cases: Replace the use of traditional passwords for authentication by acquiring and deploying appropriate multi-factor authentication for all high risk use cases and users with write/modify-rights to sensitive data	**Protect**	Standards for credentials for gaining access to IT resources are formally defined and governed by enterprise policy with senior management oversight. Policy identifies specific management and administrative roles and responsibilities, including applicability to vendors and contractors, and is applied and enforced comprehensively for all use cases and platforms in the enterprise IT asset inventory. Policy enforcement addresses requirements applicable to levels of authentication assurance for systems and data commensurate with business processes and impact of risk exposure. Standards address password strength as applicable to assurance requirements, and are based on industry-accepted standards for consumer authentication. Traditional passwords have been replaced by multi-factor credentials for all high risk use cases including remote access users, privileged users and administrators (i.e., users authorized to bypass or modify security controls and device or data configurations), and users with write/modify-rights to sensitive data. Credentials are administered and managed through enterprise provisioning process. Standards are further enforced and enhanced through a program of regular and periodic review, maintenance, update, and audit.	**5305.4** Personnel Management **5360** Identity and Access Management **5360.1** Remote Access	**Access Control:** **AC-1** ACCESS CONTROL POLICY AND PROCEDURES **AC-2** ACCESS CONTROL POLICY AND PROCEDURES **AC-17** REMOTE ACCESS **Identification and Authentication:** **IA-1** IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES **IA-2** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) **IA-2 (1)** Network Access to Privileged Accounts **IA-2 (2)** Network Access to Non-Privileged Accounts **IA-2 (3)** Local Access to Privileged Accounts **IA-2 (4)** Local Access to Non-Privileged Accounts **IA-4** IDENTIVER MANAGEMENT **IA-5** AUTHENTICATOR MANAGEMENT **IA-8** IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) **Personnel Security:** **PS-5** Personnel Transfer **PS-6** Access Agreements
		Privileged User Management and Best Practices Enforcement: Enhance the administration of privileged accounts (i.e., users authorized to bypass or modify security controls and device or data configurations) by acquiring and deploying appropriate Privileged Account Management solution. Configure and systematically enforce expiration of all privileged accounts. Consider the implementation of a shared-account password management capability	**Protect**	Approach for user access authorization rights and privilege management is defined and governed as part of the enterprise IAM policy. Authorization management practices are managed through enterprise provisioning process, enforced through enterprise authoritative identity data sources, and integrated with centralized access management processes and technology. Execution of authentication rights and privileges are contingent on successful authentication, and are comprehensively used to facilitate reduced sign-on, role and entitlement management, and transaction monitoring as applicable. Authorization management enforcement is strengthened through regular and periodic re-validation of individual user access requirements and assignments. Processes and integrity of authorization data is enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.	**5305.4** Personnel Management **5360** Identity and Access Management **5360.1** Remote Access	**Access Control:** **AC-1** ACCESS CONTROL POLICY AND PROCEDURES **AC-2** ACCOUNT MANAGEMENT **AC-6** LEAST PRIVILEGE **AC-17** REMOTE ACCESS **Identification and Authentication:** **IA-1** IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES **IA-5** AUTHENTICATOR MANAGEMENT **IA-11** RE-AUTHENTICATION

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
MOBILE SECURITY	**Deploy appropriate management and protection controls on mobile devices that will maintain stated security objectives for hosted data and applications under specific use cases, establish minimal controls for protecting devices, and enforce location-based policies with respect to applicable information, network, and application architectures.**	**Enterprise Mobile Device Management**: Establish and document a formal enterprise security policy and standards for mobile handheld devices and device configuration management	**Protect**	Devices configurations are formally defined and governed by enterprise policy.	**5350.1** Encryption **5365.3** Media Disposal **5315.5** Configuration Management	**Access Control:** **AC-19** ACCESS CONTROL FOR MOBILE DEVICES **Configuration Management:** **CM-2** BASELINE CONFIGURATION **Identification and Authentication:** **IA-3** DEVICE IDENTIFICATION AND AUTHENTICATION
				Configurations are enforced through comprehensive device management technologies that include configuration control and remote wipe; data transmission and on-device encryption; data archiving and containerization; on-device application control and enterprise mobile application lifecycle management; user authentication to device and device authentication to environment.		
				Training on appropriate use is included in regular and periodic security awareness program.		
				Monitoring and reporting processes are defined and established to ensure policy adherence.		
				Device configurations and protections are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		

SIMM 5300-B FOUNDATIONAL FRAMEWORK

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
SECURITY ANALYTICS AND CONTINUOUS MONITORING	**Deploy controls that monitor and prevent attacks or limit the consequences of their success on the network or within the infrastructure.**	**Exposure and Intrusion Detection and Prevention Capability**: Deploy monitoring and response processes and technologies for all inbound, internal, and outbound network activity to identify suspicious patterns and correct malicious or unauthorized actions or policy violations	**Detect**	Modern, enterprise-class network intrusion prevention/detection technologies are deployed and operational to provide feedback on protection of critical IT resources and business processes with significant sensitive information responsibilities. Solution(s) are: aligned with organization-specific business processes; tailored commensurate with enterprise data classification policy; aligned and integrated with enterprise telecommunications and network services strategy as well as the network zoning strategy. Monitoring capabilities include: critical alert escalation through enterprise incident response process; supplementation with active network segment blocking, re-routing, or resource suspension; integration with enterprise security information and event management (SIEM) capability and/or security operations center (SOC). Monitoring effectiveness is maintained through a program of regular and periodic review, update, and audit. A baseline of activity within the organization has been created from which anomalous activity can be identified and investigated. Baseline maintenance is part of the development lifecycle and revalidated as part of the testing new services. Signature based tools are used at appropriate choke points within the organization to identify malicious activity embedded in valid traffic flows. There is a well defined incident response process when anomalous activity is detected, which includes a pre-defined action plan and a communication plan for key stakeholders.	**5335.1** Continuous Monitoring **5335** Information Security Monitoring **5335.2** Auditable Events **5340** Information Security Incident Management **5340.3** Incident Handling **5340.4** Incident Reporting	**Audit and Accountability:** **AU-2** AUDIT EVENTS **AU-3** CONTENT OF AUDIT RECORDS **AU-6** AUDIT REVIEW, ANALYSIS, AND **Reporting:** **AU-7** LOG AGGREGATION **AU-12** AUDIT GENERATION **Incident Response:** **IR-4** INCIDENT HANDLING **IR-1** INCIDENT RESPONSE POLICY AND PROCEDURES **IR-5** INCIDENT RESPONSE MONITORING **System and Information Integrity:** **SI-3** MALICIOUS CODE PROTECTION **SI-4** INFORMATION SYSTEM MONITORING
		Enterprise Specific Event Correlation and Evaluation Capability: Acquire and deploy organization-specific event analysis capabilities for critical infrastructure environments and those with significant sensitive information contents. Consider engaging a Managed Security Service Provider (MSSP) to assist in monitoring and analyzing system events	**Detect**	Organization-specific Security Information and Event Management (SIEM) risk monitoring capabilities are deployed for critical infrastructure environments and those with significant sensitive information contents. SIEM integrates and archives alert and transaction log information from all critical perimeter and infrastructure processing, monitoring, and control devices. Alerts are integrated with organization-specific incident response process. Risk monitoring and analytics processes and technologies are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.	**5335.1** Continuous Monitoring **5335** Information Security Monitoring **5335.2** Auditable Events **5355.2** Security Alerts, Advisories, and Directives	**Audit and Accountability:** **AU-2** AUDIT EVENTS **AU-3** CONTENT OF AUDIT RECORDS **AU-6** AUDIT REVIEW, ANALYSIS, AND REPORTING **AU-7** LOG AGGREGATION **AU-12** AUDIT GENERATION **Incident Response:** **IR-4** INCIDENT HANDLING **System and Information Integrity**: **SI-3** MALICIOUS CODE PROTECTION **SI-4** INFORMATION SYSTEM MONITORING **SI-5** SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
NETWORK SECURITY	**Deploy controls that establish external perimeters to separate zones of trust (enterprise-wide, business unit/function, location) and to enforce controls on the traffic entering or leaving each zone.**	**Technical Enforcement of Security Layers and Data Center Separation**: Create multiple distinct zones separated by firewall functionality. Deploy technical security separation controls (e.g., firewall-enforced network segmentation) between user resources and infrastructure (e.g., servers, mainframes, network components) resources located on the internal, trusted network (data center firewall)	**Protect**	Comprehensive standards for internal telecommunication network architecture are formally defined and governed by enterprise policy with senior management oversight.	**5315.8** Information Asset Connections **5350** Operational Security	**System and Communications Protection:** **SC-7** BOUNDARY PROTECTION **Security Assessment and Authorization:** **CA-3** SYSTEM INTERCONNECTIONS
				Standards include identification and definition of zones of trust including perimeter zones such as De-Militarized Zones, Trusted Zones such as user and resource zones, and Restricted Zones such as high-value asset, Control, or Audit Zones.		
				Standards address authorized internal network protocols, zone perimeter configurations, and protection and monitoring controls commensurate and aligned with enterprise data classification and telecommunications and network services policies and standards.		
				Authorized use case guidelines for each zone are defined and enforced, and include the protection of data and resources used, processed, stored, or transmitted through the zone.		
				Standards are enforced through integration of modern network segmentation technologies and methodologies into enterprise perimeter control and monitoring infrastructure.		
				Standards and zoning architecture are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		
		Network Admission Control: Establish enterprise policy and practices for establishing connections with the IT infrastructure that includes identification and definition of connection types used throughout the enterprise in alignment with business processes	**Detect**	Comprehensive endpoint connection and remote access strategy is formally defined and governed by enterprise policy with senior management oversight.	**5315.8** Information Asset Connections **5355.1** Malicious Code Protection **5360.1** Remote Access **5360.2** Wireless Access **5315.5** Configuration Management **5360** Identity and Access Management	**Security Assessment and Authorization:** **CA-2** SECURITY ASSESSMENTS **CA-5** PLAN OF ACTION AND MILESTONES **CA-6** SECURITY AUTHORIZATION **CM-7** LEAST FUNCTIONALITY **Program Management:** **PM-4** PLAN OF ACTION AND MILESTONES PROCESS **PM-9** RISK MANAGEMENT STRATEGY **PM-10** SECURITY AUTHORIZATION PROCES
				Strategy includes identification and definition of authorized business-justified remote access use cases, and identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Strategy is aligned and integrated with enterprise telecommunications and network services policy, as well as device configuration management strategy.		
				Policy and practices for establishing connections with the IT infrastructure includes identification and definition of connection types used throughout the enterprise in alignment with business processes.		
				Authorized use case guidelines for connection approaches include remote, wired, wireless, and other over-the-air, as well as required standards for security and data protection per use case.		
				Secure access policy enforces: standards for user and device identification and authentication; device configuration with respect to operating system, patch level, anti-malware software, endpoint protection mechanisms, and telecommunications capabilities; device health with respect to unauthorized or malicious software.		
				Implementation is enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		

SIMM 5300-B FOUNDATIONAL FRAMEWORK

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
PHYSICAL SECURITY	**Ensure that a defense-in-depth approach includes physical controls that protect against unauthorized access to or inadvertent exposure of critical IT equipment and sensitive information.**	**Physical Security Policy Enforcement for Data Center and Remote Sites**: Evaluate and enforce existing physical security policies and practices through monitoring and audit reporting	**Protect**	Comprehensive physical protection and access strategy is formally defined and governed by enterprise policy with senior management oversight.	**5365** Physical Security **5365.1** Access Control for Output Devices **5365.2** Media Protection **5365.3** Media Disposal **5320.4** Personnel Security	**Identification and Authentication:** **IA-2** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) **Media Protection:** **MP-2** MEDIA ACCESS **MP-4** MEDIA STORAGE **Physical and Environmental Protection**: **PE-1** PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES **PE-2** PHYSICAL ACCESS AUTHORIZATIONS **PE-3** PHYSICAL ACCESS CONTROL **PE-5** ACCESS CONTROL FOR OUTPUT DEVICES **PE-6** MONITORING PHYSICAL ACCESS **PE-18** LOCATION OF INFORMATION SYSTEM COMPONENTS
				Strategy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Strategy is commensurate with business use cases and aligned with business and security objectives.		
				Policy is enforced through comprehensive hybrid of modern technological and procedural methods which address: hazard free building location (airports, nuclear power plants); building perimeter and interior access controls; visitor and vendor control and logging; locking office space and printer protection; hardcopy protection including retention, storage, destruction, and "clean desk"; video surveillance for internal, perimeter, and external; emergency procedures; personnel badging and key access.		
				Policy and practices enforcements are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		

SIMM 5300-B FOUNDATIONAL FRAMEWORK

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
VULNERABILITY MANAGEMENT	**Deploy controls to track and map assets to technical security policy, monitor and scan for known vulnerabilities, and evaluate and mitigate vulnerabilities by patching the software, changing configurations, or deploying other controls in an attempt to reduce the attack surface at the resource layer (system or device operating systems, applications, databases, and other information technology (IT) resources).**	**Comprehensive Platform-Specific Anti-Malware Approach**: Deploy anti-malicious software or endpoint protection solution on all server and workstation platforms used across the enterprise	**Protect**	Comprehensive anti-malicious software strategy is formally defined and governed by enterprise security management policy.	**5355** Endpoint Defense **5355.1** Malicious Code Protection **5355.2** Security Alerts, Advisories, and Directives	**System and Information Integrity:** **SI-3** MALICIOUS CODE PROTECTION **SI-3 (1)** Central Management **SI-3 (2)** Automatic Updates **SI-4** INFORMATION SYSTEM MONITORING **SI-4 (2)** Automated Tools for Real-Time Analysis **SI-4 (5)** System Generated Alerts
				Policy identifies process-specific operational, management, and administrative roles and responsibilities including applicability to vendors and contractors.		
				Strategy is commensurate with business use cases and aligned with business and security objectives.		
				Anti-malicious software/endpoint protection solutions are deployed on all server and workstation platforms used across the enterprise, including mobile devices.		
				Enterprise class Secure Web Gateway (SWG) and Secure Email Gateway are deployed to filter critical infrastructure environments from malicious software, external attacks, and other inappropriate or unauthorized activity.		
				Solution(s) are aligned with organization-specific business processes and tailored commensurate with enterprise acceptable use and data classification policies.		
				Prevention controls are enforced with active blocking and alerting.		
				Deployment is comprehensive across all server platform types including application, file share, data base and data repository, communication and collaboration, and domain management.		
				Deployment encompasses all platforms in all environments including external and internal-facing, production, development, test, and stand-alone.		
				Solutions are configured to accept timely updates to attack recognition criteria or signature information, as well as processing and analysis engine software.		
				Solution is configured for centralized alerting and notification, and integrated with security event management or security operations center, and incident response and management processes.		
				Control effectiveness is enhanced and validated through a program of regular and periodic review, maintenance, update, testing, and audit.		
		Comprehensive Incident Response and Management Plan: Establish repeatable and consistent enterprise policy, processes, and practices for security incident response and management	**Respond**	Comprehensive security incident handling strategy is formally defined and governed by enterprise policy with senior management oversight.	**5340** Information Security Incident Management **5340.2** Incident Response Testing **5340.3** Incident Handling **5340.4** Incident Reporting	**Incident Response:** **IR-1** INCIDENT RESPONSE POLICY AND PROCEDURES **IR-2** INCIDENT RESPONSE TRAINING **IR-3** INCIDENT RESPONSE TESTING **IR-4** INCIDENT HANDLING **IR-5** INCIDENT MONITORING **IR-6** INCIDENT REPORTING **IR-8** INCIDENT RESPONSE PLAN
				Policy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Incident response and management plan is documented and includes identification and definition of potential and actual incident events and associated priorities, responses, authority, roles and responsibilities, points of escalation, and closure.		
				Plan identifies security-specific technical, operational, management and administrative roles and responsibilities, including applicability to vendors and contractors.		
				Plan includes communication plan that addresses emergency notification, management escalation, peer and partner notification, public affairs communication management, and constituent (service/product customer/consumer) notification with respect to applicable statutory regulations.		
				Incident handling process, governed by the plan, addresses event reporting intake and coordination, immediate incident response and triage, near-term vulnerability remediation and testing, long-term enterprise architecture enhancement, tracking and reporting events metrics and lessons learned, and formal closure.		
				Incident handling processes is integrated with and escalation to business continuity, disaster recovery, and emergency management plans as appropriate.		
				Incident response and management plan is maintained through a program of regular and periodic formal reviews and testing, as well as personnel training.		

Security Program Framework [REPORT at this level]	GOALS	2016 2018 PRIORITY OBJECTIVES [MANAGE at This Level]	NIST CYBER SECURITY FUNCTION	TARGET STATE [What Good Looks Like]	SAM 5300 REFERENCE [DEPLOY at This Level]	NIST 800 53 REFERENCE (Control Family, Number, Name)
VULNERABILITY MANAGEMENT, CONT.			**Respond**	Incident reporting process is addressed through enterprise security awareness program.		
				Incident response and management plan and processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		
		Comprehensive Platform-Specific Vulnerability Patching Process: Establish a formal, comprehensive organization-specific platform management process to ensure that vendor platform operating system and software releases and patches are appropriately identified, evaluated, tested, and deployed in a timely manner for all IT assets in use by or managed on behalf of the organization (patch management process)	**Protect**	Patch management standards are formally defined and governed by enterprise configuration management policy with senior management oversight.	**5305.8** Provisions for Agreements with State and Non-State Entities **5345** Vulnerability and Threat Management **5355.2** Security Alerts, Advisories, and Directives	**Configuration Management:** **CM-2** BASELINE CONFIGURATION **System and Services Acquisition:** **SA-10** DEVELOPER CONFIGURATION MANAGEMENT **SA-22** UNSUPPORTED SYSTEM COMPONENTS **System and Information Integrity**: **SI-2** FLAW REMEDIATION
				Policy identifies specific management and administrative roles and responsibilities, including dependencies of vendors and contractors.		
				Standards address all platform and 3rd-party software.		
				Processes are used to ensure that applicable vendor platform operating system, software releases, patches are appropriately identified, evaluated, tested, and deployed in a timely manner for all IT assets in use by or managed on behalf of the organization.		
				Processes includes testing in target or like environment, and deployment to individual devices through a controlled process from a managed distribution environment.		
				Patch management is enforced through metrics related to successful testing and deployment, and include closed-loop follow-up verification of successful deployment.		
				Patch management tools include automated patch management solution, and integrate tracking through organization-specific change management process.		
				Patch management processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		
		Comprehensive Vulnerability Identification Program Including Periodic and Pre-Production Vulnerability Scans for Platforms and Applications: Establish a formal, comprehensive enterprise vulnerability scanning and testing program that includes regular and periodic vulnerability scanning of all operational applications, platforms, and devices operating in production as well prior to placing any applications, platforms, or devices into production	**Detect**	Vulnerability management practices are formally defined, documented, and governed by enterprise configuration management policy with senior management oversight.	**5345** Vulnerability and Threat Management **5355.2** Security Alerts, Advisories, and Directives	**Risk Assessment Policy and Procedures**: **RA-5** VULNERABILITY SCANNING **System and Services Acquisition:** **SA-11** DEVELOPER SECURITY TESTING AND EVALUATION **System and Information Integrity:** **SI-2** FLAW REMEDIATION **SI-7** SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
				Policy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.		
				Comprehensive enterprise vulnerability scanning and testing program includes regular and periodic vulnerability scanning of all operational applications, platforms, and devices operating in production as well as prior to placing any applications, platforms, or devices into production.		
				Pre-production vulnerability scanning is used to supplement all software and hardware build, promotion, and production-release processes.		
				The scanning program is enforced at both the enterprise and organization-specific levels, as well as from both external and internal perspectives.		
				Vulnerability scanning program is supplemented with additional program of regular and periodic active penetration testing.		
				Critical or repeat findings are escalated to enterprise level for tracking and reporting.		
				Enforce policy for remediation of critical, externally-determined findings within specific period of time with defined consequences for lack of compliance.		
				Integrate remediation of scan and test findings with organization-specific change management process.		
				Vulnerability scanning processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.		