<table>
<thead>
<tr>
<th>Security Program Framework</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE</th>
<th>SAM 5300 REFERENCE</th>
<th>NIST 800-53 REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REPORT] at this level</td>
<td>[MANAGE] at this level</td>
<td>[DEPLOY at this level]</td>
<td>[What Looks Like]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 these 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.
- 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.
- 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.
- Application assurance levels have been formally defined, documented and governed through enterprise application development policy with senior management oversight.
- 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.
- 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.
- Practices are defined, documented, integrated, and enforced across all system development environments.
- Application 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.

**SAM 5300 REFERENCE**

- 5305.5 Information Asset Management
- 5315.3 Information Asset Documentation
- 5315.7 Software Usage Restrictions

**NIST 800-53 REFERENCE**

- CM-8 INFORMATION SYSTEM COMPONENT INVENTORY
- PM-5 INFORMATION ASSET INVENTORY
- GA-8 SECURITY ENGINEERING PRINCIPLES
- GA-13 DEVELOPER SECURITY TESTING AND EVALUATION
- CM-7 LEAST FUNCTIONALITY
- SI-10 INFORMATION INPUT VALIDATION

---

*JUNE 2017*
<table>
<thead>
<tr>
<th>Security Program Framework</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE</th>
<th>SAM 5300 REFERENCE</th>
<th>NIST 800-53 REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REPORT at this level]</td>
<td>[MANAGE at this level]</td>
<td>[DEPLOY at this level]</td>
<td>[WHAT GOOD LOOKS LIKE]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONTINGENCY PLANNING</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploy controls to prevent unauthorized loss of customer, critical and sensitive information. In keeping with a systematic and comprehensive security program, deploy controls to protect information availability.</td>
<td>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).</td>
<td>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.</td>
<td>NIST 5325 Business Continuity with Technology Recovery</td>
<td>5325.1 Technology Recovery Plan</td>
<td>5325.4 Alternate Storage and Processing Site</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Impact Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>Testing is conducted 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 failure and recovery testing for all systems supporting critical business processes.</td>
<td>NIST 5325 Business Continuity with Technology Recovery</td>
<td>5325.3 Technology Recovery Testing</td>
<td>5325.6 Information System Backups</td>
<td></td>
</tr>
<tr>
<td>Comprehensive DRP Testing:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing disaster recovery processes to include periodic live testing of recovery capabilities and incorporating feedback to refine the processes.</td>
<td>Test results are used as feedback to the plan review process and incorporated as refinements to the plan.</td>
<td>NIST 5325 Business Continuity with Technology Recovery</td>
<td>5325.3 Technology Recovery Testing</td>
<td>5325.6 Information System Backups</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comprehensive DRP Testing:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Existing disaster recovery processes to include periodic live testing of recovery capabilities and incorporating feedback to refine the processes.</td>
<td>Test results are used as feedback to the plan review process and incorporated as refinements to the plan.</td>
<td>NIST 5325 Business Continuity with Technology Recovery</td>
<td>5325.3 Technology Recovery Testing</td>
<td>5325.6 Information System Backups</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Change and Configuration Management

<table>
<thead>
<tr>
<th>Goals</th>
<th>Objectives</th>
<th>NIST Cyber Security Function</th>
<th>Target State</th>
<th>Sam 5300 Reference</th>
<th>Nist 800-53 Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Practices are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>Enterprise policy is comprehensively applied across the enterprise; mandates the maintenance of an enterprise change management process; 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.</td>
<td>Implementation includes the use of automation for workflow, cataloging, tracking, and reporting.</td>
<td>Monitoring and reporting processes are defined and established to ensure policy adherence.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>Establish comprehensive enterprise change management process, workflow, and database.</td>
<td>Implement configuration management: CM-3 configuration management, CM-4 security impact analysis, CM-5 access restrictions for change.</td>
<td>Identify</td>
<td>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.</td>
<td>Configuration Management: CM-3 configuration management, CM-4 security impact analysis, CM-5 access restrictions for change.</td>
</tr>
</tbody>
</table>
## Security Program Framework

### Goals

- 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.

- Business data use cases and practices are formally defined and governed by enterprise policy with senior management oversight.

- 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 hardware 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.

- An 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.

### Target State

- 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 personal information by programs and information systems.

- 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 auditing.

- All public websites contain a Privacy Policy Statement. All online and hard copy forms that collect personal information contain a Notice on Collection.

### Reference

- NIST SP 800-53 Reference

<table>
<thead>
<tr>
<th>FOUNDATIONAL FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Program Framework</strong></td>
</tr>
<tr>
<td><strong>[REPORT level]</strong> at this <strong>[MANAGE Level]</strong> at This</td>
</tr>
<tr>
<td><strong>DATA SECURITY</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>GOALS</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>REPORT at this level</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
| | | Prot...
<table>
<thead>
<tr>
<th>GOALS</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE</th>
<th>SAM 5300 REFERENCE</th>
<th>NIST 800-53 REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REPORT] at this level</td>
<td>[MANAGE] Level</td>
<td>[Prototype] at This Level</td>
<td>[What Good Looks Like]</td>
<td>[Deploy at This Level]</td>
<td>[Control Family, Number, Name]</td>
</tr>
<tr>
<td>SECURITY GOVERNANCE</td>
<td>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.</td>
<td>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.</td>
<td>Regular and periodic security awareness training is mandated by enterprise security policy with senior management oversight.</td>
<td>5305.4 Personnel Management</td>
<td>NIST 800-53 (Control Family, Number, Name)</td>
</tr>
<tr>
<td></td>
<td>Awareness Training Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Respond</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise security policy is defined with senior management accountability.</td>
<td>5305 Information Security Program</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy is defined to support achievement of security objectives communicated with business objectives.</td>
<td>5305.2 Policy, Procedures, and Standards Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy is regularly and periodically reviewed and updated for alignment with current providing industry practices and applicable threats.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy updates are regularly and periodically communicated to personnel with regard to applicability and enforcement.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comprehensive Security Policy Structure:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Formally establish and document a consolidated, comprehensive enterprise-specific security governance policy structure that includes policy, requirements, and supporting standards.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Awareness Training Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Respond</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise security policy is defined with senior management accountability.</td>
<td>5305 Information Security Program</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy is defined to support achievement of security objectives communicated with business objectives.</td>
<td>5305.2 Policy, Procedures, and Standards Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy is regularly and periodically reviewed and updated for alignment with current providing industry practices and applicable threats.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy updates are regularly and periodically communicated to personnel with regard to applicability and enforcement.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comprehensive Security Policy Structure:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Formally establish and document a consolidated, comprehensive enterprise-specific security governance policy structure that includes policy, requirements, and supporting standards.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Program Framework</td>
<td>GOALS</td>
<td>2016-2018 PRIORITY OBJECTIVES</td>
<td>CYBER SECURITY FUNCTION</td>
<td>TARGET STATE</td>
<td>SAM 5300 REFERENCE</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------</td>
<td>-------------------------------</td>
<td>-------------------------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>[REPORT] at this level</td>
<td>[MANAGE] at This Level</td>
<td>[REST] CYBER SECURITY FUNCTION</td>
<td>[WHAT GOOD LOOKS] Like</td>
<td>[DEPLOY] at this Level</td>
<td>(Control Family, Number, Name)</td>
</tr>
<tr>
<td><strong>SECURITY GOVERNANCE, CONT.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security Management Plan:</strong> 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</td>
<td>Protect</td>
<td>Comprehensive security and risk assessment strategy is formally defined and governed by the enterprise security management policy with senior management oversight.</td>
<td>5305.1 Information Security Program Management</td>
<td>5306.6 Risk Management</td>
<td>5307.1 Security Assessments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.</td>
<td>5305.2 Risk Management</td>
<td>5307.2 Risk Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>5305.4 Risk Management</td>
<td>5307.4 Security Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The assessment process is based on an industry-accepted leading practice security framework and includes criteria for qualifying risk communicated with the business mission of the organization.</td>
<td>5305.5 Risk Management</td>
<td>5307.5 Security Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>5305.7 Risk Assessment</td>
<td>5307.7 Security Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>5305.8 Security Assessment and Authorization</td>
<td>5307.8 Security Assessment and Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assessment results are provided as input into overall enterprise risk and compliance management processes.</td>
<td>5305.9 Security Assessment and Authorization</td>
<td>5307.9 Security Assessment and Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security and risk assessment processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td>5305.10 Security Assessment and Authorization</td>
<td>5307.10 Security Assessment and Authorization</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Acceptance:</strong> 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</td>
<td>Identify</td>
<td>Comprehensive security planning and system authorization strategy is formally defined and governed by the enterprise security management policy with senior management oversight.</td>
<td>5305.6 Risk Management</td>
<td>5305.7 Risk Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.</td>
<td>5305.8 Risk Management</td>
<td>5305.9 Security Authorization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>5305.10 Risk Management</td>
<td>5305.11 Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy defines and accounts 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.</td>
<td>5305.12 Risk Management</td>
<td>5305.13 Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security plans align established security policy with applicable business-specific processes.</td>
<td>5305.14 Risk Management</td>
<td>5305.15 Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>5305.16 Risk Management</td>
<td>5305.17 Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>5305.18 Risk Management</td>
<td>5305.19 Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security planning and system authorization processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td>5305.20 Risk Management</td>
<td>5305.21 Risk Management</td>
<td></td>
</tr>
</tbody>
</table>

**REFERENCES**

- NIST 800-53 Reference: [NIST 800-53](https://csrc.nist.gov/publications)
<table>
<thead>
<tr>
<th>Security Program Framework</th>
<th>GOALS</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE (What Good Looks Like)</th>
<th>SAM 5300 REFERENCE (DEPLOY at This Level)</th>
<th>NIST 800-53 REFERENCE (Control Family, Number, Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement and Acquisition</td>
<td>Protect</td>
<td>Procurement governance is formally established, including the identification of spend thresholds, and governed by enterprise policy.</td>
<td>Protect</td>
<td>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.</td>
<td>5300.4 Principles for IT Procurement</td>
<td>Access Control: AC-20 USE OF EXTERNAL INFORMATION SYSTEMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy is aligned to the strategic business objectives and articulates the business value.</td>
<td>Protect</td>
<td>Procurement process workflow is documented to illustrate how stakeholders acquire IT systems/services.</td>
<td>5305.8 Provisions for Agreements with State and Non-State Entities</td>
<td>Personnel Security: PS-7 THIRD-PARTY PERSONNEL SECURITY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procurement process workflow is documented to illustrate how stakeholders acquire IT systems/services.</td>
<td>Protect</td>
<td>Process includes incorporation of security-specific requirements commensurate with the type (hardware, software, services) and level of assurance of items being acquired.</td>
<td>5315 Information Security Integration</td>
<td>System and Services Acquisition: SA-9 EXTERNAL INFORMATION SYSTEM SERVICES</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procurement decisions are documented for transparency, and the results are commensurate with established policy.</td>
<td>Protect</td>
<td>Procurement process is periodically assessed, improvement areas identified, and enhancements implemented.</td>
<td>5330 Information Security Compliance</td>
<td>SA-10 DEVELOPER CONFIGURATION MANAGEMENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procurement process is periodically assessed, improvement areas identified, and enhancements implemented.</td>
<td>Protect</td>
<td>Procurement process is periodically assessed, improvement areas identified, and enhancements implemented.</td>
<td>5330.1 System and Services Acquisition</td>
<td>SA-4 ACQUISITION PROCESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procurement process is periodically assessed, improvement areas identified, and enhancements implemented.</td>
<td>Protect</td>
<td>Procurement process is periodically assessed, improvement areas identified, and enhancements implemented.</td>
<td></td>
<td>SA-4 (1) Functional Properties of Security Controls</td>
</tr>
<tr>
<td>Security Program Framework</td>
<td>GOALS</td>
<td>2016-2018 PRIORITY OBJECTIVES</td>
<td>NIST CYBER SECURITY FUNCTION</td>
<td>TARGET STATE (What Looks Like)</td>
<td>SAM 5300 REFERENCE (Deploy at This Level)</td>
<td>NIST 800-53 REFERENCE (Control Family, Number, Name)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
<td>--------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>[REPORT at this level]</td>
<td>[MANAGE]</td>
<td>Platform-Specific Build Standards and Procedures: Establish enterprise policy that directs the development and maintenance of organization-specific platform development / build standards, processes, and procedures</td>
<td>Protect</td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENDPOINT SECURITY</td>
<td></td>
<td>Policy identifies specific management and administrative roles and responsibilities, including dependencies of vendors and contractors.</td>
<td>Protect</td>
<td>Practices include the application of security configuration hardening requirements that are based on industry-accepted standards for platform security configuration management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Practices include the application of security configuration hardening requirements that are based on industry-accepted standards for platform security configuration management.</td>
<td>Protect</td>
<td>Practices are applied comprehensively for all platform (hardware and operating system) types in the organization IT asset inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy and standards align with and complement business-specific processes related to IT platform use.</td>
<td>Protect</td>
<td>Security hardening requirements are enforced through a program of regular and periodic review, maintenance, update, and audit.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>Protect</td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>Protect</td>
<td>Practices include the application of security configuration hardening requirements that are based on industry-accepted standards for platform security configuration management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>Protect</td>
<td>Practices are applied comprehensively for all platform (hardware and operating system) types in the organization IT asset inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>Protect</td>
<td>Policy and standards align with and complement business-specific processes related to IT platform use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Platform development / build standards, processes, and procedures are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>Protect</td>
<td>Security hardening requirements are enforced through a program of regular and periodic review, maintenance, update, and audit.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Platform-Specific Build Standards and Procedures:**
Establish enterprise policy that directs the development and maintenance of organization-specific platform development / build standards, processes, and procedures.

**Platform-Specific Hardening Standards and Procedures:**
Establish and document formal enterprise security policy and standards for platform configuration management including requirements for security configuration (hardening).

**Configuration Management:**
CM-2 BASELINE CONFIGURATION
CM-2 (1) Reviews and Updates
CM-3 CONFIGURATION CHANGE CONTROL

**Configuration Management:**
CM-6 CONFIGURATION SETTINGS

**NIST 800-53 Reference:**
535.6 Activate Only Essential Functionality
535.2 Auditable Events
535.8 Configuration Management
535.6 Activate Only Essential Functionality
535.8 Endpoint Defense
<table>
<thead>
<tr>
<th>Security Program Framework at this</th>
<th>GOALS</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>MOST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE</th>
<th>WHAT GOALS Like</th>
<th>SAM 5300 REFERENCE</th>
<th>NIST 800-53 REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REPORT] level at this</td>
<td></td>
<td>[MANAGE Level] at This</td>
<td></td>
<td></td>
<td></td>
<td>Deploy at This Level</td>
<td>(Control Family, Number, Name)</td>
</tr>
</tbody>
</table>

**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.

**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.

**Privileged User Management and Best Practice Enforcement**

Enhance the administration of privileged accounts (i.e., users authorized to bypass or modify security controls or device or data configurations) by acquiring and deploying appropriate Privileged Account Management solutions. Configure and systematically enforce expiration of all privileged accounts. Consider the implementation of a shared account password management capability.

** ønset 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 workflows, and centralized access authentication and authorization processes.

**Access Control**

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.

**NIST 800-53 REFERENCE**

S505.4 Personnel Management

S506.1 Remote Access

**PROJECT**

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 administration (i.e., users authorized to bypass or modify security controls or 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.

**ACCESS MANAGEMENT**

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 processes, enforced through enterprise authoritative identity data sources, and integrated with centralized access management processes and technology.

Exclusions of authentication rights and privileges are contingent on successful authentication, and are comprehensively used to facilitate reduced sign-on, role 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.

**REFERENCE**

NIST 800-53 REFERENCE

SAM 5300 REFERENCE

**FONDATIONAL FRAMEWORK**

Like

What Good Looks

Access Control: AC-1 ACCESS CONTROL POLICY AND PROCEDURES

AC-1 (1) Account Management

AC-1 (2) Remote of Temporary/Emergency Accounts

AC-1 (3) Disable Inactive Accounts

AC-1 (4) Automated Audit Actions

AC-2 ACCOUNT MANAGEMENT

AC-5 ACCESS ENFORCEMENT

AC-6 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)

Personal Security:

PS-3 PERSONNEL SCREENING

PS-5 PERSONNEL TRANSFER

PS-6 ACCESS AGREEMENTS

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 (2) Network Access to Privileged Accounts

IA-2 (3) Local Access to Privileged Accounts

IA-2 (4) Local Access to Non-Privileged Accounts

IA-4 IDENTIFIER MANAGEMENT

IA-5 AUTHENTICATOR MANAGEMENT

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Personal Security:

PS-3 PERSONNEL SCREENING

PS-5 PERSONNEL TRANSFER

PS-6 ACCESS AGREEMENTS

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

<table>
<thead>
<tr>
<th>Security Program Framework</th>
<th>GOALS</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE (What Good Looks Like)</th>
<th>SAM 5300 REFERENCE (Deploy at This Level)</th>
<th>NIST 800-53 REFERENCE (Control Family, Number, Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOBILE SECURITY</td>
<td>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.</td>
<td>Enterprise Mobile Device Management: Establish and document a formal enterprise security policy and standards for mobile handheld devices and device configuration management.</td>
<td>Protect</td>
<td>Devices configurations are formally defined and governed by enterprise policy. 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$500.1 Encryption</td>
<td>$505.3 Media Disposal</td>
<td>$513.5 Configuration Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5315.5 Configuration Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

JUNE 2017
<table>
<thead>
<tr>
<th>GOALS</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE (What Good Looks Like)</th>
<th>SAM 5300 REFERENCE (Deploy at This Level)</th>
<th>NIST 800-53 REFERENCE (Control Family, Number, Name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REPORT at this level]</td>
<td>[MANAGE at this level]</td>
<td>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.</td>
<td>Expose 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.</td>
<td>Detect</td>
<td>5335.1 Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td>5335 Information Security Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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).</td>
<td></td>
<td></td>
<td>5335.2 Auditable Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring effectiveness is maintained through a program of regular and periodic review, update, and audit.</td>
<td></td>
<td></td>
<td>540 Information Security Incident Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A baseline of activity within the organization has been created from which anomalous activity can be identified and investigated.</td>
<td></td>
<td></td>
<td>5340.3 Incident Handling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Baseline maintenance is part of the development lifecycle and revalidated as part of the testing new services.</td>
<td></td>
<td></td>
<td>5340.4 Incident Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signature based tools are used at appropriate choke points within the organization to identify malicious activity embedded in valid traffic flows.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organization-specific Security Information and Event Management (SIEM) risk monitoring capabilities are deployed for critical infrastructure environments and those with significant sensitive information contents.</td>
<td></td>
<td></td>
<td>5335.1 Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIEM integrates and archives alert and transaction log information from all critical perimeter and infrastructure processing, monitoring, and control devices.</td>
<td></td>
<td></td>
<td>5335 Information Security Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alerts are integrated with organization-specific incident response process.</td>
<td></td>
<td></td>
<td>5335.2 Auditable Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk monitoring and analytics processes and technologies are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td></td>
<td></td>
<td>5335.3 Security Alerts, Advisories, and Directives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit and Accountability: AU-2 AUDIT EVENTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU-3 CONTENT OF AUDIT RECORDS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IR-4 INCIDENT HANDLING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IR-5 INCIDENT RESPONSE MONITORING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>System and Information Integrity: SI-3 MALICIOUS CODE PROTECTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI-4 INFORMATION SYSTEM MONITORING</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

JUNE 2017
<table>
<thead>
<tr>
<th>Security Program Framework</th>
<th>GOALS</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE</th>
<th>SAM 5300 REFERENCE</th>
<th>NIST 800-53 REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REPORT at this level]</td>
<td>GOAL 1</td>
<td>[MANAGE at This Level]</td>
<td>[What Good Looks Like]</td>
<td>[DEPLOY at This Level]</td>
<td>System and Communications Protection: SC-7 BOUNDARY PROTECTION</td>
<td>Security Assessment and Authorization: CA-2 SECURITY ASSESSMENTS</td>
</tr>
<tr>
<td>Technical Enforcement of Security Layers and Data Center Segregation</td>
<td>Protect</td>
<td>Comprehensive standards for internal telecommunication network architecture are formally defined and governed by enterprise policy with senior management oversight.</td>
<td>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.</td>
<td>Protect</td>
<td>Protect</td>
<td>Protect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>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.</td>
<td>Protect</td>
<td>Protect</td>
<td>Protect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standards are enforced through integration of modern network segmentation technologies and methodologies into enterprise perimeter control and monitoring infrastructure.</td>
<td>Standards and zoning architecture are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td>Protect</td>
<td>Protect</td>
<td>Protect</td>
</tr>
<tr>
<td></td>
<td>Detect</td>
<td>Comprehensive-endpoint connection and remote access strategy is formally defined and governed by enterprise policy with senior management oversight.</td>
<td>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.</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strategy is aligned and integrated with enterprise telecommunication and network services policy, as well as device configuration management strategy.</td>
<td>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.</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
<td>Authorized 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.</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implementation is enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td>Implementation is enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td>Detect</td>
<td>Detect</td>
<td>Detect</td>
</tr>
</tbody>
</table>

**NIST 800-53 REFERENCES**
- 5315.5 Configuration Management
- 5301 Malicious Code Protection
- 5302 Remote Access
- 5303.2 Wireless Access
- 5305.1 Information Asset Connections
- 5305.5 Identity and Access Management
- 5355.1 Malicious Code Protection
- 5360.1 Remote Access
- 5360.2 Wireless Access
- 5315.5 Configuration Management
- 5300 Operational Security
<table>
<thead>
<tr>
<th>Security Program Framework</th>
<th>2016-2018 PRIORITY OBJECTIVES</th>
<th>NIST CYBER SECURITY FUNCTION</th>
<th>TARGET STATE</th>
<th>SAM 5300 REFERENCE</th>
<th>NIST 800-53 REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>REPORT at this level</td>
<td>GOALS [MANAGE Level] at This</td>
<td>FOUNDATIONAL FRAMEWORK</td>
<td>[What Good Looks Like]</td>
<td>(Control Family, Number, Name)</td>
<td></td>
</tr>
<tr>
<td>PHYSICAL SECURITY</td>
<td>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.</td>
<td>Physical Security Policy Enforcement for Data Center and Remote Sites: Evaluate and enforce existing physical security policies and practices through monitoring and audit reporting</td>
<td>Protect Comprehensive physical protection and access strategy is formally defined and governed by enterprise policy with senior management oversight.</td>
<td>5305 Physical Security</td>
<td>Identification and Authentication: IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strategy identifies security-specific management and administrative roles and responsibilities including applicability to vendors and contractors.</td>
<td>5305.1 Access Control for Output Devices</td>
<td>Media Protection: MP-2 MEDIA ACCESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strategy is commensurate with business use cases and aligned with business and security objectives.</td>
<td>5305.2 Media Protection</td>
<td>MP-4 MEDIA STORAGE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
<td>5305.3 Media Disposal</td>
<td>Physical and Environmental Protection: PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy and practices enforcement is enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td>5320.4 Personnel Security</td>
<td>PE-2 PHYSICAL ACCESS AUTHORIZATIONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PE-3 PHYSICAL ACCESS CONTROL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PE-5 ACCESS CONTROL FOR OUTPUT DEVICES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PE-6 MONITORING PHYSICAL ACCESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS</td>
</tr>
<tr>
<td>Security Program Framework</td>
<td>2016-2018 PRIORITY OBJECTIVES</td>
<td>NIST CYBER SECURITY FUNCTION</td>
<td>TARGET STATE</td>
<td>SAM 5300 REFERENCE</td>
<td>NIST 800-53 REFERENCE</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------</td>
<td>----------------------------</td>
<td>--------------</td>
<td>---------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>[REPORT at this level]</td>
<td>GOALS</td>
<td>[MANAGE at This Level]</td>
<td></td>
<td></td>
<td>[DEPLOY at This Level]</td>
</tr>
<tr>
<td></td>
<td>[WHAT GOALS LIKE]</td>
<td></td>
<td></td>
<td></td>
<td>[CONTROL FAMILY, NUMBER, NAME]</td>
</tr>
<tr>
<td></td>
<td>VULNERABILITY MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td>System and Information Integrity:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5.3.1 Malicious Code Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5.3.2 Security Alerts, Advisories, and Directions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Incident Handling:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.1 Incident Response Policy and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.2 Incident Response Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.3 Incident Response Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.4 Incident Handling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.5 Incident Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.6 Incident Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.8 Incident Response Plan</td>
</tr>
</tbody>
</table>

**Foundational Framework**

**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.

**Comprehensive Incident Response and Management Plan**

Establish repeatable and consistent enterprise policy, processes, and practices for security incident response and management.

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3</td>
<td>Malicious Code Protection</td>
<td>5.3.1</td>
<td>Security Alerts, Advisories, and Directions</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Incident Handling</td>
<td>6.1</td>
<td>Incident Response Policy and Procedures</td>
</tr>
<tr>
<td>6.2</td>
<td>Incident Response Training</td>
<td>6.3</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>6.3</td>
<td>Incident Response Testing</td>
<td>6.4</td>
<td>Incident Handling</td>
</tr>
<tr>
<td>6.4</td>
<td>Incident Handling</td>
<td>6.5</td>
<td>Incident Monitoring</td>
</tr>
<tr>
<td>6.5</td>
<td>Incident Monitoring</td>
<td>6.6</td>
<td>Incident Reporting</td>
</tr>
<tr>
<td>6.6</td>
<td>Incident Reporting</td>
<td>6.8</td>
<td>Incident Response Plan</td>
</tr>
</tbody>
</table>

**GOALS**

Like:

**What Good Looks Like**

**Target State**

Comprehensive anti-malicious software strategy is formally defined and governed by enterprise security management policy.

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. | 535.1 Malicious Code Protection |
| Prevention controls are enforced with active blocking and alerting. | 535.2 Security Alerts, Advisories, and Directions |
| Deployment is comprehensive across all server platform types including application, file share, data base and data repository, communication and collaboration, and domain management. | Incident Response: |
| Deployment encompasses all platforms in all environments including external and internal-facing, production, development, test, and stand-alone. | 6.1 Incident Response Policy and Procedures |
| Solutions are configured to accept timely updates to attack recognition criteria or signature information, as well as processing and analysis engine software. | 6.2 Incident Response Training |
| Solution is configured for centralized alerting and notification, and integrated with security event management or security operations center, incident response and management processes. | 6.3 Incident Response Testing |
| Control effectiveness is enhanced and validated through a program of regular and periodic review, maintenance, update, testing, and audit. | 6.4 Incident Handling |

**Objectives**

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. | 535.1 Malicious Code Protection |
| Prevention controls are enforced with active blocking and alerting. | 535.2 Security Alerts, Advisories, and Directions |
| Deployment is comprehensive across all server platform types including application, file share, data base and data repository, communication and collaboration, and domain management. | Incident Response: |
| Deployment encompasses all platforms in all environments including external and internal-facing, production, development, test, and stand-alone. | 6.1 Incident Response Policy and Procedures |
| Solutions are configured to accept timely updates to attack recognition criteria or signature information, as well as processing and analysis engine software. | 6.2 Incident Response Training |
| Solution is configured for centralized alerting and notification, and integrated with security event management or security operations center, incident response and management processes. | 6.3 Incident Response Testing |
| Control effectiveness is enhanced and validated through a program of regular and periodic review, maintenance, update, testing, and audit. | 6.4 Incident Handling |

**NIST 800-53 REFERENCE**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3</td>
<td>Malicious Code Protection</td>
<td>5.3.1</td>
<td>Security Alerts, Advisories, and Directions</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Incident Handling</td>
<td>6.1</td>
<td>Incident Response Policy and Procedures</td>
</tr>
<tr>
<td>6.2</td>
<td>Incident Response Training</td>
<td>6.3</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>6.3</td>
<td>Incident Response Testing</td>
<td>6.4</td>
<td>Incident Handling</td>
</tr>
<tr>
<td>6.4</td>
<td>Incident Handling</td>
<td>6.5</td>
<td>Incident Monitoring</td>
</tr>
<tr>
<td>6.5</td>
<td>Incident Monitoring</td>
<td>6.6</td>
<td>Incident Reporting</td>
</tr>
<tr>
<td>6.6</td>
<td>Incident Reporting</td>
<td>6.8</td>
<td>Incident Response Plan</td>
</tr>
</tbody>
</table>

**SAM 5300 REFERENCE**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.38</td>
<td>Information Security Incident Management</td>
<td>5.3.8.2</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>5.3.8.3</td>
<td>Incident Handling</td>
<td>5.3.8.4</td>
<td>Incident Reporting</td>
</tr>
</tbody>
</table>

**System and Information Integrity**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1</td>
<td>Malicious Code Protection</td>
<td>5.3.2</td>
<td>Security Alerts, Advisories, and Directions</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Incident Handling</td>
<td>6.1.1</td>
<td>Incident Response Policy and Procedures</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Incident Response Training</td>
<td>6.3.1</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>6.4.1</td>
<td>Incident Handling</td>
<td>6.5.1</td>
<td>Incident Monitoring</td>
</tr>
<tr>
<td>6.6.1</td>
<td>Incident Reporting</td>
<td>6.8.1</td>
<td>Incident Response Plan</td>
</tr>
</tbody>
</table>

**Incident Response**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1.1</td>
<td>Incident Response Policy and Procedures</td>
<td>5.3.1.2</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>5.3.1.3</td>
<td>Incident Handling</td>
<td>5.3.1.4</td>
<td>Incident Reporting</td>
</tr>
</tbody>
</table>

**Incident Handling**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1.1</td>
<td>Incident Response Policy and Procedures</td>
<td>5.3.1.2</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>5.3.1.3</td>
<td>Incident Handling</td>
<td>5.3.1.4</td>
<td>Incident Reporting</td>
</tr>
</tbody>
</table>

**Incident Response Testing**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1.1</td>
<td>Incident Response Policy and Procedures</td>
<td>5.3.1.2</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>5.3.1.3</td>
<td>Incident Handling</td>
<td>5.3.1.4</td>
<td>Incident Reporting</td>
</tr>
</tbody>
</table>

**Incident Reporting**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1.1</td>
<td>Incident Response Policy and Procedures</td>
<td>5.3.1.2</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>5.3.1.3</td>
<td>Incident Handling</td>
<td>5.3.1.4</td>
<td>Incident Reporting</td>
</tr>
</tbody>
</table>

**Incident Handling**

<table>
<thead>
<tr>
<th>Control</th>
<th>Family</th>
<th>Number</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1.1</td>
<td>Incident Response Policy and Procedures</td>
<td>5.3.1.2</td>
<td>Incident Response Testing</td>
</tr>
<tr>
<td>5.3.1.3</td>
<td>Incident Handling</td>
<td>5.3.1.4</td>
<td>Incident Reporting</td>
</tr>
<tr>
<td>Security Program Framework</td>
<td>2016-2018 PRIORITY OBJECTIVES</td>
<td>NIST CYBER SECURITY FUNCTION</td>
<td>TARGET STATE</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>GOALS</td>
<td>[REPORT at this level]</td>
<td>[MANAGE Level]</td>
<td>[What Looks Like]</td>
</tr>
<tr>
<td>Respond</td>
<td>Incident reporting process is addressed through enterprise security awareness program.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td>Patch management standards are formally defined and governed by enterprise configuration management policy with senior management oversight.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patch management tools include automated patch management solution, and integrate tracking through organization specific change management process.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td>Vulnerability management practices are formally defined, documented, and governed by enterprise configuration management policy with senior management oversight.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-production vulnerability scanning is used to supplement all software and hardware build, promotion, and production-release processes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability scanning program is supplemented with additional program of regular and periodic active penetration testing.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical or repeat findings are escalated to enterprise level for tracking and reporting.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforce policy for remediation of critical, externally determined findings within specific period of time with defined consequences for lack of compliance.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrate remediation of scan and test findings with organization specific change management process.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability scanning processes are enhanced and validated through a program of regular and periodic review, maintenance, update, and audit.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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).

**Comprehensive Vulnerability Specification 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 as prior to placing any applications, platforms, or devices into production.