Independent Security Assessment Criteria

Phase – I Version 1.1, dated 6/17/2016

For: **{Organization name}**

Performed on: **{Date of Assessment}**

Security Assessment Overview

Summary of Changes:

Item	Page	As Read	Changed to	Date
All	All	Migration from RC3 to Final Version	All requested changes in RC1, RC2 formatting changes adopted, moved to final version	3/28/2016
Score	3	Example score Calculation	Updated percentages, clarified formula conversion to %	5/5/2016
Misc	Title	Information Security Assessment	Independent Security Assessment	6/17/2016

General:

In accordance with Assembly Bill 670, enacted on October 6, 2015 Agencies are required to undergo an Independent Security Assessment in accordance with the agreed upon standards set forth by the California Information Security Office. This criterion details the areas of assessment, components evaluated, and standards for compliance determination. Assessed agencies may achieve one of three possible scores for each sub-component.

Rating	Narrative	Criteria
I	Implemented	Indicates the Organization met or exceeded the established required criteria established for evaluated component
P	Partially Implemented	Implemented indicates the Organization is not able to provide sufficient evidence to achieve an "I" rating, but has demonstrated an ongoing and active effort to achieve the "I" rating
N	Not Implemented	Represents the Organization is not able to provide evidence of even a partial implementation of the evaluated component
Note: All "P" and "N" events will require a POA&M to be filed in accordance with SIMM 5305B and 5305C within 30 days of close-out report delivery		

Scoring of Sub-Components

Each Section consists of one or more scored sub-section metrics. The total number of sub-section metrics will be counter (e.g. 5). Each sub-section rating of "I" will be scored at a Value of 2; each "P" scored as 1; and each "N" scored as 0. The total values for each (I,P, and N) will be summed together, then divided by the subsection total metrics category count. This will derive a simple Percentage. The percentage will be represented using the following value precision format (NN.NN), no rounding will be conducted.

Example:

Subsection Metric #	Sub-section Score	Converted Value
1	I	**2**
2	I	**2**
3	P	**1**
4	P	**1**
5	I	**2**
6	N	**0**

Example:

Step 1: Subsection to Score Formula: { (I * 3)= 6 + (P * 2)=2 + (N * 1)=0 } ***8*** {Subsection total Score}

Step 2: {Subsection Count} **6** / **8** (Subsection Total) = **75%**

Overall Score

The Overall Score will be an aggregate of the sum of all Section Values Divided by the # of Assessed Sections. This will derive a simple Percentage. The percentage will be represented using the following value precision format (NN.NN), no rounding will be conducted.

Example:

Access Control (AC)	*96.58*
Awareness and Training (AT)	*87.65*
Audit and Accountability (AU)	*74.95*
Security Assessment and Authorization (CA)	*95.50*
Configuration Management (CM)	*88.68*
Contingency Planning (CP)	*100.00*
Identification and Authentication (IA)	*98.65*
Incident Response (IR)	*75.25*
Maintenance (MA)	*n/a*
Media Protection (MP)	*100.00*
Physical and Environmental Protection (PE)	*n/a*
Planning (PL)	*n/a*
Program Management (PM)	*n/a*
Personnel Security (PS)	*98.50*
Risk Assessment (RA)	*94.75*
System and Services Acquisition (SA)	*n/a*
System and Communications Protection (SC)	*100.00*
System and Information Integrity (SI)	*89.97*

Calculation Steps:

Step 1: Add scores from all Applicable Sections: 1200.48

Step 2: Determine # Applicable Sections: 13

Step 3: Multiply the Applicable Sections * 100 (Max possible score): 1300

Step 4: Divide Total Applicable Sections Total / Max Possible Score: 1200.48/1300 = 0.923446154

Step 5: Convert outcome to a percentage

Step 6: Post the Overall Score: **92.34%**

Distribution of Results:

As directed by Assembly Bill 670, enacted on October 6, 2015 a copy of the Organization finding will be securely delivered to the assessed Organization, the California Office of Information Security (CISO), and the California Office of Emergency Services (Cal OES). It is the responsibility of the Organization to retain an inspection copy of the findings for future requirements, including but not limited to CISO Auditing purposes.

Dynamic Assessment Variables

Sample Set Sizing Standards:

In controls where a sample set is surveyed, the size of the sample set unless specified in the assessment documentation is determined by the designated size of the organization. For the assessment purpose, the measurement of determination is the user account population stored in the directory server (e.g. Active Directory). Once a count is performed by the assessment team, the below correlation table will be used to determine the assessment variable value:

Organization AD Population	Size Classification Category	Sample Set Size
1 - 500	Small	20
501 - 5000	Medium	50
5001 +	Large	100

Independent Security Assessment (ISA) Summary – By NIST Control Family

Family	Score	# Sub-Controls	Tested Controls	Compliance Percentage
Access Control (AC)		11	AC-3, AC-6(1), AC-6(2), AC-6(5), AC-7, AC-7(1), AC16(5), AC-17(2), AC20(1)	
Awareness and Training (AT)		3	AT-2(1), AT-2(2), AT-4	
Audit and Accountability (AU)		2	AU-11, AU-12	
Security Assessment and Authorization (CA)		2	CA-3, CA-7, AC-8(2)	
Configuration Management (CM)		7	CM-2, CM-3, CM-6, CM-7, CM-8, CM-8(1)	
Identification and Authentication (IA)		3	IA-5(1), [IA-5(2) or IA-5(11)]	
Incident Response (IR)		1	IR-6	
Media Protection (MP)		1	MP-7	
Personnel Security (PS)		1	PS-6	
Risk Assessment (RA)		4	RA-2, RA-3, RA-5, RA-5(1)	
System and Communications Protection (SC)		3	SC-7, SC-7(4), SC-7(5), SC-7(15)	
System and Information Integrity (SI)		5	SI-3(1), SI-3(2), SI-4, SI-5, SI-10	

Overall Assessment Score:_____

Assessment Collections

ID	Task	Reference	Metric	I/P/N Recap	Remarks
1	External Information System Interconnections	NIST 800-53, Control(s): AC-20(1), CA-3	Assess controls related to terms, conditions, and trust relationships with other external organizations information systems accessing backend processes and data stores; employs a Deny All, Allow by Exception (DAPE) access controls	# I # P # N	Subtasks in collection: 2 *Note: If Not Applicable, score as "n/a" and Adjust overall score as applicable*
2	User-based Training and Recording Requirements	NIST 800-53, Control(s): AT-2(2), PS-6	Organization provides cybersecurity awareness training; Training addresses Insider Threats; and Training is documented	# I # P # N	Subtasks in collection: 2
3	Information Security Training Records Management	NIST 800-53, Control(s): AT-4	Organization conducts, documents, and retails information security user awareness training	# I # P # N	Subtasks in collection: 1
4	Simulated Cyber Attack Practical Exercise	NIST 800-53, Control(s): AC-3, AC-7, AC-7(1), AT-2, CA-8(2), SI-4	Organization performs practical exercise to evaluate effectiveness of simulated cyber attack	# I # P # N	Subtasks in collection: 5
5	Information System Audit Record Generation and Retention	NIST 800-53, Control(s): AC-16(5), AU-11, AU-12 SAM 5335.2	Organization retains audit records for after-the-fact investigations of security incidents	# I # P # N	Subtasks in collection: 3

ID	Task	Reference	Metric	I/P/N Recap	Remarks
6	Organization establishes a Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support state entity risk management decisions	NIST 800-53, Control(s): CA-7	Organization maximizes the value of security controls and risk awareness through conduct of a continuous monitoring process	# I # P # N	Subtasks in collection: 1
7	Information System Lifecycle Accountability Tracking	NIST 800-53, Control(s): CM-8, CM-8(1)	Perform accountability assessment of organization owned systems lifecycle tracking	# I # P # N	Subtasks in collection: 2
8	Secure Configuration and Hardening Management and Configuration Control Monitoring, Documentation, and Deviation Procedures	NIST 800-53, Control(s): AC-6(1), AC-6(5), CM-2, CM-3, CM-6, IA-5(1), [IA-5(2) or IA-5(11) as appl] SAM 5303.5, 5315.5	Organization documents a policy, process, procedure, and application method for Secure Configuration Management; Standardized baseline system hardening in accordance with NIST 800-53 standards; and Change Control Management	# I # P # N	Subtasks in collection: 8
9	Least Functionality Configurations	NIST 800-53, Control(s): AC-6(2), CM-7, MP-7	System configuration set to only required Ports, Protocols, and secure access methods	# I # P # N	Subtasks in collection: 3
10	Incident Response Plan (IRP) Required Component Assessment	NIST 800-53, Control(s): IA-5(1), IR-6	Organization develops, reviews, updates Incident Response Plan to align with required NIST elements and SAM components	# I # P # N	Subtasks in collection: 2
11	Information Security Remote Access Compliance and Reporting	NIST 800-53, Control(s): AC-17(2), AC-20(1), SC-7(4) SAM 5360.1	Assess submission of core Information Security components as directed by SAM Chapter 5300	# I # P # N	Subtasks in collection: 2

ID	Task	Reference	Metric	I/P/N Recap	Remarks
12	Information Systems are categorized in accordance with FIPS 199; Federal / State Law; Policies; Directives; and Orders	NIST 800-53, Control(s): RA-2 SAM 5305.5	Organization reviews, reassesses, and documents the security categorization decisions and risk assessment results for all information systems under their control	# I # P # N	Subtasks in collection: 2
13	Boundary Monitoring and Protection	NIST 800-53, Control(s): CM-7, SC-7. SC-7(5), SC-7(15)	Restrict external network access using layered perimeter security, enforced monitoring, and Permit-All-Deny-by-Exception (DAPE) traffic control	# I # P # N	Subtasks in collection: 4
14	Dissemination of Alerts, Advisories, and Directives	NIST 800-53, Control(s): SI-5	Establishes effectively sharing cybersecurity alerts, advisories, directives, and intelligence within organizational stakeholders	# I # P # N	Subtasks in collection: 1
15	Organization vulnerability scanning information systems; hosted applications to enumerate software flaws; improper; and measure vulnerability impacts and remediation success	NIST 800-53, Control(s): RA-5, RA-5(1)	Organization scans for vulnerabilities, misconfigurations, assesses impacts; shares results with system administration; internal auditors; CIO/ISO; and measures success of remediation efforts	# I # P # N	Subtasks in collection: 2
16	Malicious Code Protection Policy, Process, and Procedure	NIST 800-53, Control(s): SI-3(1), SI-3(2)	Employs and maintains updated centralized malicious code protection mechanisms to detect, alert, and neutralize malicious code	# I # P # N	Subtasks in collection: 2
17	Information Input Validation (Public Web)	NIST 800-53, Control(s): SI-10	Assess Input protections of primary public web site to ensure accurate and correct inputs protections, resistance to Cross-Site Scripting (XXS), and Injection attacks	# I # P # N	Subtasks in collection: 1

Access Control (AC)

Task 1.1	Condition	Standard	Result	Remarks
Review organization's Minimum Security Requirements for Interconnection Policy AC-20(1)	Interconnect agreement includes the following minimum requirements: - Requirements contained in a formal signed agreement (SLA, MOA, IAA, contract, etc…) - Assets in agreement are classified under FIPS 199 - Minimum identified security controls mapped to NIST 800-53 / and Risk Assessment	**I –** Interconnect agreement contains all required components **P –** Interconnect missing 1 of the required components **N** – Policy or practice absent of > 1 component missing		*Note: If no external interconnections, mark as "n/a" see Task 1.*

Task 4.2	Condition	Standard	Result	Remarks
Assess organization's "Unauthorized Logon Attempt" Policy and logical implementation AC-7	Review policy and logical controls to validate implementation in the following areas: - Policy addresses failed attempt limit - Policy does not allow > 5 consecutive failed attempts - Implementation of logical controls for failed attempt limit matches policy - Policy addresses attempt delay or account lockout requirements Implementation of logical controls for attempt delay / lockout matches policy	**I –** Policy locks account after a maximum of 5 consecutive failed attempts prompt is delayed **P –** Policy locks account after 6 or more attempts, does not delay logon prompt **N** – Policy does not lock account or delay prompt		
Task 4.3	**Condition**	**Standard**	**Result**	**Remarks**
Validate Unauthorized Logon Attempt implementation AC-7(1)	Tester coordinates with directory administration team to utilize 1 random user-level account for testing. Using an authorized information systems connected to the network tester attempts: - Presentation of valid user name and 5 attempts using an incorrect password (e.g. "*4wrongOne@*") within a period of 2 minutes (or until lockout notification) - Network directory notifies user account is disabled or locked	**I –** Policy locks account after a maximum of 5 consecutive failed attempts prompt is delayed **P –** Policy locks account after 6 or more attempts, does not delay logon prompt **N** – Policy does not lock account or delay prompt		

Task 5.1	Condition	Standard	Result	Remarks
Assets Security Attributes – Standard Naming Conventions AC-16(5)	Organization establishes a Policy or Standard Operating Procedure (SOP) and practice for the standardization of logical assets as part of the method of identifying unauthorized devices on logical segments	**I –** Organization Policy SOP requiring standardization of logical asset naming conventions **P –** Organization informally standardizes on logical asset naming conventions, but no formal standard is documented **N** – Organization does not standardize on logical asset naming standards and no policy or SOP exists		
Task 8.1	**Condition**	**Standard**	**Result**	**Remarks**
Review organization's Principal of Least Privilege Policy regarding privileged account restrictions AC-6(5)	Organization policy review includes: - Policy signed by current designee - Specific prohibition regarding granting Privileged Role rights (e.g. local administrator) to standard users is contained within policy	**I –** Organizational policy signature matches appropriate designee; Policy prohibits privileged role rights assigned to standard users **P –** Policy prohibits privileged role rights assigned to standard users; Signatory is a not the current designee or document is expired **N** – Policy lacks privileged role assignment restrictions for users or no policy exists		*Note: Organization to provide a copy of the current SIMM 5330-A on file at CDT CISO office as the authoritative document for review. If document is > 12 months old, consider expired*

Task 8.2	Condition	Standard	Result	Remarks
Assess 20 random assets (see below): 1 Domain Controller 2 Application Servers 1 Database Servers 5 User Workstations 2 Admin Wrkstations 5 User Laptops 2 Admin Laptops 2 Exec Laptops review primary role privileged rights context AC-6(5)	User level accounts and privileged access rights should be provisioned as different accounts as a matter of the Principal of Least Privilege configuration. Validate the primary privileged user role for each core system to determine of standard user accounts are present.	I –All inspected roles are absent of standard user accounts. P – Between 1-2 standard user accounts demonstrated privileged access roles within the sample set. N – More than 2 standard user accounts demonstrated privileged access roles within the sample set.		Note: If origination does not have a server in one of the listed categories, substitute for a differ server type. For workstations and Laptops use the local administrator or SUDO roles (as appl)
Task 8.3	**Condition**	**Standard**	**Result**	**Remarks**
Inspect the following privileged rights roles within the directory server (as appl.): 1. Enterprise Admin 2. DNS Admin 3. Group Policy Creators 4. Account Operators 5. Backup Operators 6. Root 7. Sudoers AC-6(1)	As a matter of the Principal of Least Privilege configuration user level accounts are not role members of privileged user groups/roles. Privileged rights are exercised via 'Run as' or Sudo	**I –**All inspected privileged roles are absent of standard user accounts. **P –** Between 1-2 standard user accounts detected in privileged roles. **N** – More than 2 standard user accounts detected in privileged roles.		

Task 9.1	Condition	Standard	Result	Remarks
Least Privilege – Separation of Privileged Roles from Non-Privileged User Accounts AC-6(2)	Select 10 random organization privileged roles: - Roles should be a combination of Active Directory and NIX-based assets - Seek standard user account assigned within the role	**I –** 0 detected standard user accounts assigned privileged roles **P –** Between 1 - 2 detected standard user accounts assigned privileged roles **N –** More than 2 detected standard user accounts assigned privileged roles		
Task 11.1	**Condition**	**Standard**	**Result**	**Remarks**
Use of External Information Systems – Bring Your Own Device (BYOD) Information System Policy and Restrictions AC-20(1)	Review Organizational BYOD policy to determine: - Does organization have a policy to address BYOD - Does policy authorize use for official business - Does policy allow of interconnection to organizational provided resources (network, non-public applications, etc…) - Determine if users must sign an additional Acceptable Use Policy (AUP) - Determine if users must sign a SIMM 5360-A submission	**I –** Organization policy either allows personally owned equipment and designated stringent cyber security criteria or disallows use and prohibits connection via logical controls **P –** Organization policy allows connection but cyber security controls were not demonstrated **N –** No policy presented and a lack of preventative controls exists		

Task 11.2	Condition	Standard	Result	Remarks
Remote Access – Integrity using Encryption AC-17(2), SC-7(4), SAM 5360.1	Validate that Network-Level connections from external networks (VPN) require FIPS 140-2 approved encryption as a requirement of connection establishment	**I –** All network-level connections require an encrypted VPN Tunneled protections secured communication channel using approved FIPS 140-2 **P –** All network-level connections require an encrypted VPN Tunneled protections secured communication channel but are not using FIPS 140-2 encryption components N – No evidence of logical requirements to enforce external network-level connections is present		Notes: **a.** If the organization does not support VPN, this rate this as n/a and decrement the total sub-assessment items for this category **b.** If an existing legacy VPN solution is in place that support FIPS 140-1, list on POA&M pending organization upgrade / replacement

Awareness Training (AT)

Task 2.1	Condition	Standard	Result	Remarks
Review organizational User-based training content to validate minimum content included AT-2(2)	Organization User Training includes as a minimum the following modules / content: 1) Disgruntled employee 2) Unauthorized material access 3) Repeat policy violators 4) Reporting standards modules	**I –** Training includes: disgruntled employee, unauthorized material access, repeat policy violators, and reporting standards. **P –** Training includes no less than 2 of the abovementioned modules **N** – Training lacks 3 or more of the identified modules		
Task 3.1	**Condition**	**Standard**	**Result**	**Remarks**
Review organization User Training artifacts AT-4	Select *random subset* of standard users & 3 organization executives. Validate training artifacts include: - Training date - User Name - Training Level (User, Admin, Exec, etc..) Pass or Fail (as appl, if knowledge assessment conducted)	**I –** Greater than 100% employees training documented and up to date (within 1 year) **P –** Organization 99% - 70% employees training documented and up to date (within 1 year) **N –** Less than 70% employees training documented and up to date (within 1 year)		Note: sample subset size based on established criteria, see pg 4.

Task 4.4	Condition	Standard	Result	Remarks
User Awareness Training – Practical Exercise AT-2(1), CA-8(2)	Organization conducts unannounced simulated phishing attempt on 100 random user email accounts (incl 3 executives) - Organization provides a complete list of active user email addresses - Organization coordinates with email administrator / provider to whitelist test domain - Organization does not inhibit phishing attempts using logical controls	**I –** Less than 5% of phished addresses successful **P –** Between 6 - 10% of phished addresses successful **N –** Greater than 11% of phished addresses successful		*Note: if Organization is less than 100 users than all users will be assessed and scored as appropriate*

Audit and Accountability (AU)

Task 5.2	Condition	Standard	Result	Remarks
Review Organization Key Event Log Retention Policy AU-11, SAM 5335.2	Organization policy specifies retention fidelity for following key audit logs: - DNS Ingress/Egress - File Server Object Access - Web Usage - Domain Controller Event - Firewall Events - IPS/IDS Events	**I –** All 6 logs are retained in accordance with organization retention policy **P –** Between 3-5 logs are retained based on organization retention policy **N** – < 3 of the required logs are retained or no retention policy for specified logs was provided		
Task 5.3	**Condition**	**Standard**	**Result**	**Remarks**
Review Organization Log Generation and Retention AU-12, SAM 5335.2	Organization policy specifies the minimum retention period for audit logs Identified in Task 5.2. Validate that logs in each category specified are being generated and retained.	**I –** Policy and practice retains key log events in accordance with Policy **P –** Policy and practice retains key service log events in accordance with Policy **N –** Policy and practice retains key log events in accordance with Policy		The following retention periods are documented per policy for the following logs: DNS Ingress/Egress: _____ File Server Obj Access: _____ Web Usage: _____ DC/GC Events: _____ Firewall Events: _____ IPS/IDS Events: _____

Security Assessment and Authorization (CA)

Task 1.2	Condition	Standard	Result	Remarks
System Interconnection Logical Documentation CA-3	Organization documents each external System interconnect via logical interface within in a network diagram	**I –** All System Interconnects documented in Security Plan and associated logical network diagram(s) **P –** Greater than 90% of Interconnects documented in Security Plan and associated diagrams **N –** Less than 89% or absence of documentation of Interconnects in Security Plan or no network diagramming present		
Task 6.1	**Condition**	**Standard**	**Result**	**Remarks**
Continuous Monitoring Program Policy and Program Implementation CA-7	Organization defines and conducts: - Policy for Continuous Monitoring (CM) of security controls - Policy for monitoring frequency - Policy for sharing detected vulnerabilities with appropriate internal key stakeholders - Establishes metrics for vulnerability resolution - Provides metric status reporting to senior organizational leaders (e.g. CIO, AIO, ISO, Governance team, etc…)	**I –** Policy defines CM requirements, frequency, and result distribution to key stakeholders; Metrics for CM resolution defined; CM metrics distribution requirements to Key senior leaders defined **P –** Policy defines CM requirements, frequency, and result distribution to key stakeholders / senior leaders; no metrics for resolution defined **N –** Absence CM policy or more than 1 component missing from policy		

Configuration Management (CM)

Task 7.1	Condition	Standard	Result	Remarks
Information System Inventory – Verification of Assets CM-8(1)	Select a random subset of organization accounts of assigned Information systems: - Host to Serial Number or Asset Tag Correlation - Ability to account for Lifecycle removal of assets - Ability to correlate responsible / assigned parties to assets - Accounts for *random subset* of assets not detected during live host scan	**I –** Organization accounts for greater than 100% of all devices **P –** Organization accounts for 99% - 90% of devices or excess unaccounted equipment present **N –** Organization accounts for < 89% of devices or excess unaccounted equipment present		Note: sample subset size based on established criteria, see pg 4.
Task 7.2	**Condition**	**Standard**	**Result**	**Remarks**
Information System Inventory – Policy Review CM-8	Organization policy details management controls: - Lifecycle tracking from acquisition through disposal - Accountable party - Current disposition of information assets - Policy updated as required or at time of responsible party change	**I –** Policy is signed by appropriate designee; Establishes asset lifecycle tracking; Identifies current responsible parties; Identified current asset disposition **P –** Policy establishes asset lifecycle tracking and Identifies current responsible party requirements but either lacks current asset disposition guidance or is not signed by appropriate designee **N –** Unable to document policy or lacks > 2 components listed		

Task 8.4	Condition	Standard	Result	Remarks
Configuration Settings – Documents and Implements configuration settings to implement system hardening and security posture CM-6, SAM 5305.5	Organization policy and practice establishes: - System minimum hardening criteria based on appropriate NIST baseline controls - Employs methods for the automated application, update, and enforcement of established baseline hardening controls - Periodically reevaluates system hardening controls against baseline images and updates as required	**I –** Policy for system hardening requires use of an established organizational baseline image; logical NIST security controls be enforced and updated using automated measures; and periodic reevaluation of image baseline for compliance with current standards **P –** Policy for system hardening requires use of an established organizational baseline image; logical NIST security controls be enforced and updated using automated measures; no documentation of baseline image review or update procedures / practices **N –** Organization does not use baseline secured image or no evidence of NIST logical control enforcement / update		

Task 8.5	Condition	Standard	Result	Remarks
Configuration Change Control – Policy, Practice, and Documentation Verification CM-3, SAM 5315.5	Organization provides previous 5 implemented configuration change actions for analysis of practices related to: - Documented Policy / Standard Operating Procedure (SOP), or practice - Documentation requires technical impact assessment and recommendation - Document requires documented approval prior to implementation Documentation is archived in accordance with organizational documentation requirements (Min 6 months)	**I –** 5 requests completed the CCB process in accordance with standards established **P -** 4 requests completed the CCB process in accordance with standards established **N –** < 4 assessed requests followed established process standards; or Absence of formal Change Control Process		
Task 8.6	**Condition**	**Standard**	**Result**	**Remarks**
Baseline Image Security Configuration and Analysis CM-2	Identify 10 production systems for System Image and Harding Analysis consisting of: - 1 Domain Controller - 3 Application Servers - 3 Workstations - 3 Laptops Assessed Conditions: a - Conduct SCAP scan using current NIST Template to determine overall compliance and hardening rating b – Ensure absence of OEM image presence on assessed asset	**I –** Combined SCAP average exceeds 75%; absence of detected OEM images **P –** Combined SCAP average exceeds 50%; absence of detected OEM images **N –** Combined SCAP average < 50%; or detection of OEM images		

Task 9.2	Condition	Standard	Result	Remarks
Least Functionality Configuration – Excessive Port and Protocol Identification CM-7	Select a *random subset* of organization systems to determine if configured to Least Functionality configuration: - Absence of excessive port listeners - Absence of insecure protocols - Unusual detected port / protocols approved by Configure Control Board (CCB) documented review	**I –** 0 detected unapproved / excessive port listeners or at risk protocols identified **P –** Between 99% – 90% of assessed systems absent of unapproved / excessive port listeners or at risk protocols identified **N –** < 89% of assessed systems absent of unapproved / excessive port listeners or at risk protocols identified		Note: sample subset size based on established criteria, see pg 4.
Task 13.1	**Condition**	**Standard**	**Result**	**Remarks**
Boundary Protection – Prohibit use of Insecure management protocols CM-7	Perimeter security device administrative management port(s) restrict insecure protocols	**I –** Only secure protocols allowed **P –** Insecure protocols only allowed from intranet designated subnets **N –** No restrictions on insecure protocol usage		

Identification and Authentication (IA)

Task 8.7	Condition	Standard	Result	Remarks
Authenticator Management – Password Based Authentication Enforcement Standards IA-5(1)	Establish 2 new test accounts in the directory: a. <u>User-level account</u>: - Attempt password reset < Policy minimum characters - Attempt password reset < policy entropy requirements - Attempt password reset by reusing prior valid password b. <u>Administrator-level account</u>: - Attempt password reset < Policy minimum characters - Attempt password reset < policy entropy requirements - Attempt password reset by reusing prior valid password	**I –** User and Administrator level account policy components all enforced via logical restrictions during password reset attempts **P –**Administrator level account policy components all enforced via logical restrictions during password reset attempts; 1 of the policy documented user-level logical restrictions failed **N –** 1 or more Administrator level account logical restrictions failed or > 1 User level logical enforcement failed		*Note: If hardware appliances are identified that do not support minimum organizational administrative requirements, ensure on POA&M for replacement / upgrade*
Task 8.8	**Condition**	**Standard**	**Result**	**Remarks**
Use of PKI or Token Based Authentication Alternative Implemented IA-5(2) or IA-5(11) as appl.	Review user account provisioning of a select *random subset* of user accounts to determine if user and administrative credentials have been replaced with token or PKI-based authentication	**I –** Organization has replaced all user and administrator logon credentials with PKI or Hardware tokens. **P –** Organization documents an active initiative in process to deploy tokens / PKI as replacement to passwords **N –** Organization not undertaking password preplacement using PKI or Token-based authentication		*Notes:* **a.** *On Final results, if (2) or (11) is applicable to the implementation, only display the applicable result; if neither default to IA-5(11)* **b.** *Sample subset size based on established criteria, see pg 4.*

Task 10.1	Condition	Standard	Result	Remarks
Authenticator Management – Policy Standards for Authentication Enforcement IA-5(1)	Review organization policy regarding the minimum standards for authentication enforcement. Ensure the following minimal requirements are implemented: - Minimum length: 8 - Entropy: Upper, Lower, Special and Numeric characters - Maximum lifetime: 6 months - Reuse Restriction: 10 prior	**I –** Organizational policy address all areas and meets or exceeds minimum identified thresholds **P –** Organizational policy requires minimum length and entropy; other requirements mission or unspecified **N –** Organizational policy requirements for minimum length or entropy does not meet requirements and more than 2 components unspecified or fail to meet minimum criteria		

Incident Response (IR)

Task 10.2	Condition	Standard	Result	Remarks
Incident Reporting Process and Procedure IR- 6	Organization documents processes for log analysis and anomalous event escalation: - To organization security team - CIO, AIO, ISO, Governance team (as appl.) - Performs formal notification to CDT-CISO, CHP once incident validated	**I –** Procedure documents clearly defined analysis, event documentation, and reporting steps **P –** Procedure documents analysis, and reporting steps; preservation of documentation not clearly defined **N –** Organization lacks a clearly defined and documented Incident handling and reporting procedures		

Media Protection (MP)

Task – 9.3	Condition	Standard	Result	Remarks
Media Use – Policy Regarding Restrictions of Non-Government Provided Removable Media and Government Media Accountability MP-7	Review organizational policy for: - Prohibitions regarding use non-government provided removal media (e.g. Flash Drives, smart phones, tablets, e-readers, etc…) - Prohibitions regarding the connection on non-government media to government owned / controller information systems - Accountability and management controls related to approved government furnished removable media	**I –** Policy details prohibitions regarding use / connection of non-government removable media to information systems; establishes strict accountability and logical controls for government owned removable media usage **P –** Policy details prohibitions regarding use / connection of non-government removable media to information systems; policy does not detail accountability and logical controls for government owned removable media usage **N –** Policy detailing non-government media usage / connection was not documented; or no logical controls were demonstrated to prohibit non-government media connection / usage		

Personnel Security (PS)

Task 2.2	Condition	Standard	Result	Remarks
Access Agreements – Validation of Program and Usage of Acceptable Use Policy (AUP) PS-6	Select a *random subset* of user accounts from the directory: - Request blank current Access Agreement (AUP) - Review each random user selected to validate current form is provided for user - Validate all random selected users form have all required sections signed - For each random user without a form, review Directory service to ensure user account disabled	**I –** Greater than 90% of random user sample is compliant **P –** Between 80-89% of random user sample is compliant **N –** 80% of random user sample is compliant		Note: Sample subset size based on established criteria, see pg 4.

Risk Assessment (RA)

Task 12.1	Condition	Standard	Result	Remarks
Security Categorization – FIPS 199 Classification Documentation RA-2, SAM 5305.	All information systems owned or controlled by the Organization are assigned an information system security classification consistent with FIPS 199 directives	**I –** All State controlled IT assets documented by classification; levels below Moderate justified **P –** Organization documents an ongoing process which is between 99 – 90% **N –** Organization does not have any documentation of by-asset classification activities documented or is less than 90% complete		
Task 12.2	**Condition**	**Standard**	**Result**	**Remarks**
Security Categorization – High Risk System Risk Mitigation Documentation RA-3	Organization maintains detailed historical assessment and Risk Mitigations related to all systems rated as “high” under FIPS 199	**I –** Organization identifies and retains historical documentation of all systems classified as “High” under FIPS 199; All Identified Risks include mitigation plans to reduce impacts **P –** Organization identifies and retains historical documentation of all systems classified as “High” under FIPS 199; Partial risk mitigation plans are implemented **N –** No evidence of High Risk assets or risk mitigation plans are documented		**Note: If organization does not have “High” systems identified in Task 12.1 then score as “n/a” and deprecate the total subtasks in score**

Task 15.1	Condition	Standard	Result	Remarks
Vulnerability Scanning – Measuring Vulnerability Impacts on Assets RA-5	Organization performs a vulnerability scan of all systems under its control: - No less than monthly - Results include detected vulnerabilities Results equate impacts to a vulnerability rating	**I –** Organization provides two consecutive prior monthly vulnerability scans of all systems; Evidence of process to conduct scans no less than monthly; Scan includes detected vulnerabilities and impact ratings **P –** Organization provides current month vulnerability scans of all systems; Evidence of process to conduct scans no less than monthly; Scan includes detected vulnerabilities and impact ratings; or provided vulnerability scan is between 2 – 12 months old but provides detected vulnerabilities and impact ratings **N –** Organization does not provide proof of an All System Vulnerability scan that includes impact rating conducted		
Task 15.2	**Condition**	**Standard**	**Result**	**Remarks**
Vulnerability Scanning – Signatures < 30 Days Old RA-5(1)	Review date of last signature update on organizational vulnerability scanner: - Update < 30 days from date of assessment	**I –** Database signatures are less than 30 days from date of assessment **P –** Database signatures between 30 to 90 days from date of assessment **N –** Signatures do not exist or older than 90 days		Note: sample subset size based on established criteria, see pg 4.

System and Communication Protection (SC)

Task 13.2	Condition	Standard	Result	Remarks
Boundary Protection – Prohibit Traversal via Non-Monitored Interface SC-7	Review network diagrams and Firewall configurations: - Validate all network ingress / egress points are documented - Validate all network traffic is logically routed through perimeter network monitoring devices	**I –** All ingress/egress points monitored **P –** 1 unmonitored ingress /egress points is present; POA&M submitted **N –** Multiple unmonitored / undocumented pathways exist on network		*Note: A result of "N" in this category is a "Critical" and must be reported to the CIO / CDT CISO immediately*
Task 13.3	**Condition**	**Standard**	**Result**	**Remarks**
Boundary Protection – Deny All, Allow by Exception Configuration Review SC-7(5)	Perform an analysis of the primary Boundary Protection Firewall rules sets to determine: - Are rules implemented using a Deny All, Allow by Exception (DAPE) configuration - Are exceptions specific to the minimal IP's and ports / protocols required - Do "any" rules exist in the External or DMZ networks	**I –** NIST Firewall Score or Overall Security Rating Greater than 75% **P –** NIST Firewall Score or Overall Security Rating Greater than between 75% and 50%. **I –** NIST Firewall Score or Overall Security Rating less than 50%		

Task 13.4	Condition	Standard	Result	Remarks
Boundary Protection – Route Privileged Network Access SC-7(15)	Review Primary Firewall configuration to determine if management interface is configured to prohibit external network access	**I –** Remote network administration access prohibited from external IP addresses **P –** Remote administration access allowed from approved external IP address assignments only with additional compensation controls (e.g. single IP point to point only; Two-Factor Authentication Protected) **N –** No restrictions on Remote administration access or missing Two-Factor protections		

System and Information Integrity (SI)

Task 4.1	Condition	Standard	Result	Remarks
Information System Monitoring – Detection and Mitigation of Rouge Devices SI-4	Organization detects and acts upon unauthorized devices on the network: - Network security team detects improperly names asset connection - Network team blocks logical access to internal network resources for unauthorized device - Network team reports incident to ISO / Security team - Device is located and removed	**I –** Organization detects, blocks logical access, reports security incident, and removes unauthorized network connection **P –** Organization detects device, reports security incident, but does not inhibit device logical access **N –** Organization does not actively monitor for rouge device detection or fails to react to rouge device detection during assessment		
Task 14.1	**Condition**	**Standard**	**Result**	**Remarks**
Security Alerts, Advisories, and Directive Dissemination SI-5	Organization policy defines content and time frames for sharing of security alerts, advisories, and directives with appropriate internal stakeholder (e.g. assigned System Admins, ISO, CIO, etc…)	**I –** Policy addresses content sharing of security related information to stakeholders, method of distribution, and time frame of issuance **P –** Policy addresses content sharing of security related information, does not specify stakeholders or time frame for redistribution **N –** Absence of documentation of Policy or Process to share security related alerts, advisories, etc…		

Task 16.1	Condition	Standard	Result	Remarks
Malicious Code Protection – Central Client Management SI-3(1)	Verify organization uses central Anti-malware client management: Validate managed clients match AD objects	**I –** 100% of expected clients under enterprise management **P –** Between 99% – 90% of expected clients under enterprise management **N –** Less than 90% of expected clients under enterprise management		
Task 16.2	**Condition**	**Standard**	**Result**	**Remarks**
Malicious Code Protection – Signature Management and Update Validation SI-3(2)	Select a random subset of anti-malware managed clients from the console: a. Client selection should represent the following percentages of the total random population: - Servers: 10% - Workstations: 50% - Laptops: 40% b. Review anti-virus signatures date c. Validate signatures < 4 days old	**I –** All Signatures < 4 days from date of review **P –** 1 of more signatures between 5 - 10 days from date of review **N –** 1 or more Signatures > 10 days from date of review		Note: Sample subset size based on established criteria, see pg 4.

Task 17.1	Condition	Standard	Result	Remarks
Information Input Validation – Primary External Website SI-10	Identify primary external web site for organization and validate: - Assessment of externally enumerable configuration does not expose insecurity - Site is protected against Cross-site Scripting (XSS) exploitation - Site is protected from Structured Query Language Injection (SQLi) exploitation	**I –** Organization can document external web apps/site XSS and SQLi testing within the past 2 years or at last major modification or upgrade **P –** Organization can document external web apps/site XSS and SQLi testing > 2 years or at last major modification or upgrade **N –** No evidence of external web apps/site XSS and SQLi testing or at last major modification or upgrade		