



HHS
Enterprise Information Security
Risk Assessment Monitoring Process
(EIS-RAMP)

October 2, 2015

v 1

Table of Contents

Table of Contents	2
1. Introduction	3
2. Purpose	3
3. Scope	3
4. Audience	4
5. Background	4
6. How To Use This Document	4
Small Workforce Operations.....	4
System Security Plan	4
Identifying the Security Control Baseline.....	5
7. Risk Assessment and Compliance Monitoring	6
8. Enterprise Information Security Controls Mapping to NIST SP 800-53 rev 4	7

1. Introduction

The Title 1, Texas Administrative Code (TAC), Chapter 202 ¹, RULE §202.24 Agency Information Security Program requires that all state agencies have an information security program consistent with the rules defined in the TAC 202 which includes protections, based on risk, for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the agency including outsourced resources to another agency, contractor, or other source (e.g., cloud computing). The program shall include periodic assessments of the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

The HHS Data Use Agreement requires that Contractor/Third Parties accessing and/or managing confidential information comply with periodic security controls compliance assessment and monitoring by HHS as required by state and federal law. Federal Law includes the Health Information Portability and Accountability Act (HIPAA) 45 CFR Part 164 and other federal regulations that require routine security risk analysis and risk management. These processes must include security control measures for reducing risk to an acceptable level as recommended by the National Institute of Standards and Technology (NIST).

For awarded contracts, the completion of the HHS Enterprise Data Use Agreement and Information Security and Privacy Initial Inquiry (SPI) satisfies an initial security risk assessment for Contractor/Third Parties.

The Information Security and Privacy Initial Inquiry (SPI) controls are the HHS minimally acceptable security controls baseline required prior to contract award for all Contractor/Third Parties that access and/or manage HHS confidential information with external Information Systems. The SPI baseline of security controls are identified in Section 8.

2. Purpose

The Enterprise Information Security Risk Assessment and Monitoring Process (EIS-RAMP) is designed to meet compliance with state and federal regulations to assess risk and accomplish the security monitoring requirement with the overall objective of reducing risk to a manageable level.

3. Scope

The EIS-RAMP applies to Contractor/Third Party external service providers that access or manage Health and Human Services (HHS) Confidential Information.

The EIS-RAMP does not apply to customers of HHS services.

¹ The Title 1, Texas Administrative Code (TAC), Chapter 202 can be found at:
[http://texreg.sos.state.tx.us/public/readtac\\$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202)

4. Audience

The EIS-RAMP is primarily intended to be used by Contractor/Third Party Information Security Officers, staff, or officials who have been designated as responsible for the organizations information security and the protection of HHS Confidential Information.

5. Background

The security controls contained in Section 8 are designed to protect and meet the security objectives of confidentiality, integrity, and availability of information for the information system, reducing risk to a manageable level.

The security controls are derived from the controls prescribed in the Texas Department of Information Resources (DIR) Security Control Standards Catalog² and the NIST Special Publication 800-53³ Revision 4 Moderate security control baseline. Reviewing these DIR and NIST documents will convey how these security controls are designed to meet the security objectives of confidentiality, integrity, and availability and protect information systems from unauthorized access, use, modification, and destruction.

6. How To Use This Document

Small Workforce Operations

Small Workforce Operations will only be required to comply with the SPI Security Controls baseline identified in Section 8 of this document.

Small Workforce Operations typically involve small, informal home office types of information technology configurations that **may** also contain the following characteristics.

- Small, independent, family-owned, controlled, and operated business
- A minimum amount of employees
- Small amount of business volume, typically not franchised, therefore open for business only in a single location.
- Small business's operated out of the primary residence of the owner(s).

System Security Plan

Following contract award, the HHS Information Owner or their designee will collaborate with the respective Agency ISO and Contractor/Third Party to identify required security controls for the information system.

² The DIR Security Control Standards Catalog can be found at: <http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Security%20Control%20Standards%20Catalog%20V1.2.docx>

³ The NIST SP 800-53 can be found at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

A System Security Plan (SSP) template, provided by the Agency ISO, will be used to document the required security controls as well as other information specific to the information system.

The SSP template will become the System Security Plan for the information system. The selection and implementation of required security controls documented in the SSP will be a risk-based approach, where 100% compliance will be achieved over time based on the control implementation timelines identified in Section 8.

Identifying the Security Control Baseline

The SSP includes a Security Categorization (SC) process to determine the correct baseline of security controls for the information system.

Small Workforce Operations will only be required to comply with the SPI Security Controls baseline identified in Section 8 of this document.

There are 3 possible SC levels identified in the SSP which are Low, Moderate or High.

The SC levels map directly to the HHS Control Baseline of Low, Moderate or High contained in Section 8 of this document. For example a SC level of high will map to a security control baseline of high.

The security control baseline will map directly to and is primarily based on the 3 data classification levels of Public, Agency Sensitive or Confidential.

Although in some cases, based on the business impact of the information system, a higher SC level and control baseline may be more necessary than the data classification requires. For example, a climate control system in a data center would be considered critical and may require a high control baseline although it does not process confidential information.

The mapping of the SC level and impact to data classification security control baseline contained in Section 8 are indicated in the following table.

Security Categorization (SC) & Impact	Regulation Drivers	Data Classification	HHS Control Baseline	Control Source
Low	TAC 202	Public	Low	TAC 202 controls catalog (Low baseline controls). Is for systems using HHS public data
Moderate	TAC 202	Agency Sensitive	Moderate	TAC 202 controls catalog (Low baseline controls) + Additional controls as necessary (SANS top 20 Critical Controls). Is for systems using HHS agency sensitive data
High	TAC 202, Federal	Confidential	High	NIST SP 800-53 Rev 4 Moderate base controls +control enhancements (TAC 202 controls catalog Moderate controls) <ul style="list-style-type: none"> Additional specific controls (e.g., HIPAA, SANS requirements mapped to NIST SP 800-53 rev4. Is for systems using HHS confidential data

7. Risk Assessment and Compliance Monitoring

Contractor/Third Parties are required to follow the risk based approach of control implementation identified in their information system SSP's, with the objective of achieving 100% compliance of control implementation based on the implementation timelines of Section 8.

HHS Information Owners are responsible for ensuring information security risk assessments are performed. The information system SSP will be the primary document for the risk assessment and compliance monitoring.

HHS Agency Information Security Officers and Information Owners will identify on an annual basis, a schedule of which systems will be assessed for compliance monitoring.

Once notified by the Agency Information Security Officer and Information Owner that a system is scheduled for assessment, the Contractor/Third Party will have 90 days to return a completed SSP.

8. Enterprise Information Security Controls Mapping to NIST SP 800-53 rev 4

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls identified below will be assessed during the HHS annual risk assessment and monitoring process. The Information Security and Privacy Initial Inquiry (SPI) controls are the HHS minimally acceptable controls required for contractors that access and/or manage HHS confidential information. For contractors with small standalone computers (Small Workforce operations), only the SPI controls are required. All other systems and contractors will also be required to comply with the LOW, MOD or HIGH baselines control according to the type of HHS data they are using or per the determined system security categorization level. At a minimum, the control baseline of LOW is for systems using HHS public data, MOD is for systems using HHS agency sensitive data, and HIGH is for systems using HHS confidential data. Compliance with these controls will be on a risk-based approach where 100% compliance will be achieved over time.

ACCESS (AC) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
AC-1	Access Control Policy and Procedures	P1	x	x	x		2015
AC-2	Account Management	P1	x	x	x	x	2015
AC-2(1)	Account Management (Automated System Account Management)	P1			x		2016
AC-2(2)	Account Management (Removal of Temporary Accounts)	P1			x		2015
AC-2(3)	Account Management (Disable Inactive Accounts)	P1			x		2015
AC-2(4)	Account Management (Automated Audit Actions)	P1			x		2015
AC-3	Access Enforcement	P1	x	x	x		2015
AC-4	Information Flow Enforcement	P1		x	x		2017
AC-5	Separation of Duties	P1		x	x		2015
AC-6	Least Privilege	P1		x	x		2017
AC-6(1)	Least Privilege (Authorize Access to Security Functions)	P1			x		2017

ACCESS (AC) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
AC-6 (2)	Non- privileged access non-security functions	P1			x		2017
AC-6 (5)	Privileged Accounts	P1			x		2017
AC-6 (9)	Auditing use of privileged functions.	P1			x		2017
AC-6 (10)	Prohibit non-privileged users from executing privileged functions	P1			x		2017
AC-7	Unsuccessful Logon Attempts	P2	x	x	x	x	2015
AC-8	System Use Notification	P1	x	x	x		2015
AC-9	Previous Logon (Access) Notification	P0					TBD
AC-10	Concurrent Session Control	P3					TBD
AC-11	Session Lock	P3		x	x	x	2015
AC-11(1)	Session Lock (Pattern-Hiding Displays)	P3			x		2017
AC-12	Session Termination	P2		x	x		2017
AC-14	Permitted Actions without Identification or Authentication	P3	x	x	x		2017
AC-16	Security Attributes	P0					TBD
AC-17	Remote Access	P1	x	x	x	x	2015
AC-17(1)	Remote Access (Automated Monitoring / Control)	P1			x		2015
AC-17(2)	Remote Access (Protection of confidentiality/integrity using encryption)	P1			x	x	2015
AC-17(3)	Remote Access (Managed access control points)	P1			x		2015
AC-17(4)	Remote Access (Privileged commands/access)	P1			x		2015

ACCESS (AC) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
AC-18	Wireless Access	P1	x	x	x	x	2015
AC-18(1)	Wireless Access (Authentication and Encryption)	P1			x	x	2015
AC-19	Access Control for Mobile Devices	P1	x	x	x		2016
AC-19(5)	Access Control for Mobile Devices (Full Device / Container-Based Encryption)	P1			x		2016
AC-20	Use of External Information Systems	P1	x	x	x		2016
AC-20(1)	Use of External Information Systems (Limits on Authorized Use)	P1			x		2016
AC-20(2)	Use of External Information Systems (Portable Storage Devices)	P1			x		2016
AC-21	Information Sharing	P2			x		TBD
AC-22	Publicly Accessible Content	P3	x	x	x		2017
AC-23	Data Mining Protection	P0					2017
AC-24	Access Control Decisions	P0					TBD
AC-25	Reference Monitor	P0					TBD

AWARENESS AND TRAINING (AT) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
AT-1	Security Awareness and Training Policy and Procedures	P1	x	x	x		2015
AT-2	Security Awareness Training	P1	x	x	x	x	2015
AT-2(2)	Security Awareness (Insider Threat)	P1			x		2015
AT-3	Role-Based Security Training	P1	x	x	x		2016
AT-4	Security Training Records	P3	x	x	x		2017

AUDIT AND ACCOUNTABILITY (AU) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
AU-1	Audit and Accountability Policy and Procedures	P1	x	x	x		2016
AU-2	Audit Events	P1	x	x	x		2015
AU-2(3)	Audit Events (Reviews and Updates)	P1			x		2015
AU-3	Content of Audit Records	P1	x	x	x		2016
AU-3(1)	Content of Audit Records (Additional Audit Information)	P1			x		2016
AU-4	Audit Storage Capacity	P1	x	x	x		2016
AU-5	Response to Audit Processing Failures	P1	x	x	x		2016
AU-6	Audit Review, Analysis, and Reporting	P1	x	x	x	x	2015

AUDIT AND ACCOUNTABILITY (AU) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
AU-6(1)	Audit Review, Analysis, and Reporting (Process Integration)	P1			x		2015
AU-6(3)	Audit Review, Analysis, and Reporting (Correlate Audit Repositories)	P1			x		2015
AU-7	Audit Reduction and Report Generation	P2		x	x		2017
AU-7(1)	Audit Reduction and Report Generation (Automatic Processing)	P2			x		2017
AU-8	Time Stamps	P1	x	x	x		2016
AU-8(1)	Time Stamps (Synchronization with Authoritative Time source)	P1			x		2016
AU-9	Protection of Audit Information	P1	x	x	x		2016
AU-9(4)	Protection of Audit Information (Access by Subset of Privileged Users)	P1			x		2016
*AU-10	Non-repudiation	P2					2017
AU-11	Audit Record Retention	P3	x	x	x		2017
AU-12	Audit Generation	P1	x	x	x		2016
AU-13	Monitoring for Information Disclosure	P0					2017
AU-14	Session Audit	P0					2017
AU-15	Alternate Audit Capability	P0					TBD
AU-16	Cross-Organizational Auditing	P0					TBD

SECURITY ASSESSMENT AND AUTHORIZATION (CA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
CA-1	Security Assessment and Authorization Policies and Procedures	P1	x	x	x		2016
CA-2	Security Assessments	P2	x	x	x		2015
CA-2(1)	Security Assessments (Independent Assessors)	P2			x		2015
CA-3	System Interconnections	P1	x	x	x		2016
CA-3 (5)	System Interconnections (Restrictions on External System Connections)	P1			x		2016
CA-5	Plan of Action and Milestones	P3	x	x	x		2017
CA-6	Security Authorization	P2	x	x	x		2017
CA-7	Continuous Monitoring	P2	x	x	x		2017
CA-7(1)	Continuous Monitoring (Independent Assessment)	P2			x		2017
CA-8	Penetration Testing	P2					TBD
CA-9	Internal System Connections	P2	x	x	x		2017

CONFIGURATION MANAGEMENT (CM) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
CM-1	Configuration Management Policy and Procedures	P1	x	x	x		2015
CM-2	Baseline Configuration	P1	x	x	x		2016
CM-2(1)	Baseline Configuration (Reviews and Updates)	P1			x		2016
CM-2(3)	Baseline Configuration (Retention of Previous Configurations)	P1			x		2016
CM-2(7)	Baseline Configuration (Configure Systems, Components, Or Devices For High-Risk Areas)	P1			x		2016
CM-3	Configuration Change Control	P1		x	x		2017
CM-3 (2)	Configuration Change Control (Test / Validate / Document Changes)	P1			x		2017
CM-4	Security Impact Analysis	P2	x	x	x		2015
CM-4(1)	Security Impact Analysis (Separate test environments)	P2			x		2015
CM-5	Access Restrictions for Change	P1		x	x		2017
CM-6	Configuration Settings	P1	x	x	x	x	2015
CM-7	Least Functionality	P1	x	x	x	x	2015
CM-7 (1)	Least Functionality (Periodic Reviews)	P1			x		2015
CM-7 (2)	Least Functionality (Prevent Program Execution)	P1			x		2015
CM-7 (4)	Least Functionality (Unauthorized Software / Blacklisting)	P1			x		2015
CM-8	Information System Component Inventory	P1	x	x	x		2016
CM-8 (1)	Information System Component Inventory (Updates During Installations / Removals)	P1			x		2016

CONFIGURATION MANAGEMENT (CM) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
CM-8 (3)	Information System Component Inventory (Automated Unauthorized Component Detection)	P1			X		2016
CM-8 (5)	Information System Component Inventory (No Duplicative Accounting of Components)	P1			X		2016
CM-9	Configuration Management Plan	P1		X	X		2017
CM-10	Software Usage Restrictions	P2	X	X	X		2017
CM-11	User-Installed Software	P1	X	X	X		2015

CONTINGENCY PLANNING (CP) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
CP-1	Contingency Planning Policy and Procedures	P1	x	x	x		2016
CP-2	Contingency Plan	P1	x	x	x		2015
CP-2 (1)	Contingency Plan (Coordinates with Related Plans)	P1			x		2015
CP-2 (3)	Contingency Plan (Resume Essential Missions / Business Functions)	P1			x		2015
CP-2 (8)	Contingency Plan (Identify Critical Assets)	P1			x		2015
CP-3	Contingency Training	P2	x	x	x		2017
CP-4	Contingency Plan Testing	P2	x	x	x		2015
CP-4 (1)	Contingency Plan Testing (Coordinate with Related Plans)	P2			x		2015
CP-6	Alternate Storage Site	P1		x	x		2015
CP-6(1)	Alternate Storage Site (Separation From Primary Site)	P1			x		2015
CP-6(3)	Alternate Storage Site (Accessibility)	P1			x		2015
CP-7	Alternate Processing Site	P1			x		TBD
CP-7 (1)	Alternate Processing Site (Separation From Primary Site)	P1			x		TBD
CP-7 (2)	Alternate Processing Site (Accessibility)	P1			x		TBD
CP-7(3)	Alternate Processing Site (Priority of Service)	P1			x		TBD
CP-8	Telecommunications Services	P1			x		TBD
CP-8 (1)	Telecommunications Services (Priority of Service Provisions)	P1			x		TBD

CONTINGENCY PLANNING (CP) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
CP-8 (2)	Telecommunications Services (Single Points of Failure)	P1			x		TBD
CP-9	Information System Backup	P1	x	x	x		2016
CP-9 (1)	Information System Backup ((Testing for Reliability / Integrity)	P1			x		2016
CP-10	Information System Recovery and Reconstitution	P1	x	x	x		2016
CP-10 (2)	Information System Recovery and Reconstitution (Transaction Recovery)	P1			x		2016
CP-11	Alternate Communications Protocols	P0					TBD
CP-12	Safe Mode	P0					TBD
CP-13	Alternative Security Mechanisms	P0					TBD

IDENTIFICATION AND AUTHENTICATION (IA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
IA-1	Identification and Authentication Policy and Procedures	P1	x	x	x		2015
IA-2	Identification and Authentication (Organizational Users)	P1	x	x	x	x	2015
IA-2 (1)	Identification and Authentication (Network Access to Privileged Accounts)	P1			x		2015
IA-2 (8)	Identification and Authentication (Network Access To Privileged Accounts - Replay Resistant)	P1			x		2015
IA-2 (11)	Identification and Authentication (Remote Access - Separate Device)	P1			x		2015
IA-3	Device Identification and Authentication	P1		x	x		2017
IA-4	Identifier Management	P1	x	x	x		2015
IA-5	Authenticator Management	P1	x	x	x	x	2015
IA-5 (1)	Authenticator Management (Password-based Authentication)	P1			x	x	2015
IA-5 (2)	Authenticator Management (PKI-based Authentication)	P1			x		2015
IA-5 (3)	Authenticator Management (In-person or Trusted Third-Party Registration)	P1			x		2015
IA-5 (11)	Authenticator Management (Hardware or Software Token-based Authentication)	P1			x		2015

IDENTIFICATION AND AUTHENTICATION (IA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
IA-6	Authenticator Feedback	P2	x	x	x		2016
IA-7	Cryptographic Module Authentication	P1	x	x	x		2016
IA-8	Identification and Authentication (Non-Organizational Users)	P1	x	x	x		2016
IA-9	Service Identification and Authentication	P0					TBD
IA-10	Adaptive Identification and Authentication	P0					2017
IA-11	Re-authentication	P0					TBD

INCIDENT RESPONSE (IR) CONTROLS

(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
IR-1	Incident Response Policy and Procedures	P1	x	x	x		2015
IR-2	Incident Response Training	P2	x	x	x		2017
IR-3	Incident Response Testing	P2		x	x		2017
IR-3(2)	Incident Response Testing (Coordinating with Related Plans)	P2			x		2017
IR-4	Incident Handling	P1	x	x	x		2016
IR-4(1)	Incident Handling (Automated Incident Handling Processes)	P1			x		2016
IR-5	Incident Monitoring	P1	x	x	x		2016
IR-6	Incident Reporting	P1	x	x	x		2015
IR-6(1)	Incident Reporting (Automated Reporting)	P1			x		2017
IR-7	Incident Response Assistance	P2	x	x	x		2017
IR-7(1)	Incident Response Assistance (Automation Support for Availability of Information / Support)	P2			x		2017
IR-8	Incident Response Plan	P1	x	x	x		2016
IR-9	Information Spillage Response	P0					2017
IR-10	Integrated Information Security Analysis Team	P0					2017

MAINTENANCE (MA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
MA-1	System Maintenance Policy and Procedures	P1	x	x	x		2016
MA-2	Controlled Maintenance	P2	x	x	x		2017
MA-3	Maintenance Tools	P3			x		2017
MA-3(1)	Maintenance Tools (Inspect Tools)	P3			x		2017
MA-3(2)	Maintenance Tools (Inspect Media)	P3			x		2017
MA-4	Nonlocal Maintenance	P2	x	x	x		2017
MA-4(2)	Nonlocal Maintenance (Document Nonlocal Maintenance)	P2			x		2017
MA-5	Maintenance Personnel	P2	x	x	x		2017
MA-6	Timely Maintenance	P2			x		TBD

MEDIA PROTECTION (MP) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
MP-1	Media Protection Policy and Procedures	P1	x	x	x		2016
MP-2	Media Access	P1	x	x	x		2016
MP-3	Media Marking	P2		x	x		2017
MP-4	Media Storage	P1		x	x	x	2015
MP-5	Media Transport	P1		x	x	x	2015
MP-5(4)	Media Transport (Cryptographic Protection)	P1			x		2015
MP-6	Media Sanitization	P1	x	x	x	x	2015
MP-7	Media Use	P1	x	x	x		2016
MP-7(1)	Media Use (Prohibit Use Without Owner)	P1			x		2016
MP-8	Media Downgrading	P0					TBD

PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
PE-1	Physical and Environmental Protection Policy and Procedures	P1	x	x	x		2015
PE-2	Physical Access Authorizations	P1	x	x	x	x	2015
PE-3	Physical Access Control	P1	x	x	x	x	2015
PE-4	Access Control for Transmission Medium	P1			x		TBD
PE-5	Access Control for Output Devices	P2			x	x	2015
PE-6	Monitoring Physical Access	P1	x	x	x		2016
PE-6(1)	Monitoring Physical Access (Intrusion Alarms / Surveillance Equipment)	P1			x		2016
PE-8	Visitor Access Records	P3	x	x	x		2017
PE-9	Power Equipment and Cabling	P1			x		TBD
PE-10	Emergency Shutoff	P1			x		TBD
PE-11	Emergency Power	P1			x		TBD
PE-12	Emergency Lighting	P1	x	x	x		2016
PE-13	Fire Protection	P1	x	x	x		2015
PE-13(3)	Fire Protection (Automatic Fire Suppression)	P1			x		2015
PE-14	Temperature and Humidity Controls	P1	x	x	x		2016
PE-15	Water Damage Protection	P1	x	x	x		2016
PE-16	Delivery and Removal	P2	x	x	x		2017
PE-17	Alternate Work Site	P2			x		TBD
PE-18	Location of Information System Components	P3					TBD
PE-19	Information Leakage	P0					TBD
PE-20	Asset Monitoring and Tracking	P0					TBD

PLANNING (PL) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
PL-1	Security Planning Policy and Procedures	P1	x	x	x		2016
PL-2	System Security Plan	P1	x	x	x		2015
PL-2(3)	System Security Plan (Plan / Coordinate With Other Organizational Entities)	P1			x		2015
PL-4	Rules of Behavior	P2	x	x	x	x	2015
PL-4(1)	Rules of Behavior/Acceptable Use (Social Media and Networking Restrictions)	P2			x	x	2015
*PL-7	Security Concept of Operations	P0					TBD
PL-8	Information Security Architecture	P1			x		TBD
*PL-9	Central Management	P0					TBD

PROGRAM MANAGEMENT (PM) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
PM-1	Information Security Program Plan	P1					2015
PM-2	Senior Information Security Officer	P1				x	2015
PM-3	Information Security Resources	P1					2015
PM-4	Plan of Action and Milestones Process	P1					2016
PM-5	Information System Inventory	P1					2016
PM-6	Information Security Measures of Performance	P1					2016
PM-7	Enterprise Architecture	P1					2016
PM-8	Critical Infrastructure Plan	P1					
PM-9	Risk Management Strategy	P1					
PM-10	Security Authorization Process	P1					
PM-11	Mission/Business Process Definition	P1					
PM-12	Insider Threat Program	P1					
PM-13	Information Security Workforce	P1					
PM-14	Testing, Training, and Monitoring	P1					
PM-15	Contacts with Security Groups and Associations	P3					
PM-16	Threat Awareness Program	P1					

PERSONNEL SECURITY (PS) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
PS-1	Personnel Security Policy and Procedures	P1	x	x	x		2016
PS-2	Position Risk Designation	P1	x	x	x		2015
PS-3	Personnel Screening	P1	x	x	x		2016
PS-4	Personnel Termination	P1	x	x	x		2016
PS-5	Personnel Transfer	P2	x	x	x		2017
PS-6	Access Agreements	P3	x	x	x		2017
PS-7	Third-Party Personnel Security	P1	x	x	x	x	2015
PS-8	Personnel Sanctions	P3	x	x	x		2017

RISK ASSESSMENT (RA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
RA-1	Risk Assessment Policy and Procedures	P1	x	x	x		2016
RA-2	Security Categorization	P1	x	x	x		2015
RA-3	Risk Assessment	P1	x	x	x		2015
RA-5	Vulnerability Scanning	P1	x	x	x		2016
RA-5(1)	Vulnerability Scanning (Update Tool Capability)	P1			x		2016
RA-5(2)	Vulnerability Scanning (Update by Frequency / Prior to New Scan / When Identified)	P1			x		2016
RA-5(5)	Vulnerability Scanning (Privileged Access)	P1			x		2016
*RA-6	Technical Surveillance Countermeasures Survey	P0					2017

SYSTEM AND SERVICES ACQUISITION (SA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
SA-1	System and Services Acquisition Policy and Procedures	P1	x	x	x		2016
SA-2	Allocation of Resources	P1	x	x	x		2016
SA-3	System Development Life Cycle	P1	x	x	x		2015
SA-4	Acquisition Process	P1	x	x	x		2016
SA-4(1)	Acquisition Process (Functional Properties of Security Controls)	P1			x		2016
SA-4(2)	Acquisition Process (Design / Implementation Information For Security Controls)	P1			x		2016
SA-4(9)	Acquisition Process (Functions / Ports / Protocols / Services in Use)	P1			x		2016
SA-5	Information System Documentation	P2	x	x	x		2017
SA-8	Security Engineering Principles	P1			x		2017
SA-9	External Information System Services	P1	x	x	x	x	2015
SA-9(2)	External Information Systems (Identification of Functions / Ports / Protocols / Services)	P1			x		2015

SYSTEM AND SERVICES ACQUISITION (SA) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
SA-9(5)	External Information Systems (Processing, Storage, and Service Location)	P1		x	x	x	2015
SA-10	Developer Configuration Management	P1		x	x		2015
SA-11	Developer Security Testing and Evaluation	P1		x	x		2017
SA-12	Supply Chain Protection	P1					TBD
SA-13	Trustworthiness	P0					2017
SA-14	Criticality Analysis	P0					TBD
SA-15	Development Process, Standards, and Tools	P2					2017
SA-16	Developer-Provided Training	P2					2017
SA-17	Developer Security Architecture and Design	P1					2017
SA-18	Tamper Resistance and Detection	P0					TBD
SA-19	Component Authenticity	P0					TBD
SA-20	Customized Development of Critical Components	P0					2017
SA-21	Developer Screening	P0					2017
SA-22	Unsupported System Components	P0					TBD

SYSTEM AND COMMUNICATIONS PROTECTION (SC) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calendar Year)
SC-1	System and Communications Protection Policy and Procedures	P1	x	x	x		2016
SC-2	Application Partitioning	P1			x		TBD
SC-3	Security Function Isolation	P1					TBD
SC-4	Information in Shared Resources	P1			x		TBD
SC-5	Denial of Service Protection	P1	x	x	x		2015
SC-6	Resource Availability	P0					TBD
SC-7	Boundary Protection	P1	x	x	x		2016
SC-7(3)	Boundary Protection (Access Points)	P1			x		2016
SC-7(4)	Boundary Protection (External Telecommunications Services)	P1			x		2016
SC-7(5)	Boundary Protection (Deny by Default / Allow by Exception)	P1			x		2016
SC-7(7)	Boundary Protection (Prevent Split Tunneling for Remote Devices)	P1			x		2016
SC-8	Transmission Confidentiality and Integrity	P1		x	x	x	2015
SC-8(1)	Transmission Confidentiality and Integrity (Cryptographic or Alternate Physical Protection)	P1			x		2015
SC-10	Network Disconnect	P2			x		TBD
SC-11	Trusted Path	P0					TBD
SC-12	Cryptographic Key Establishment and Management	P1	x	x	x		2016
SC-13	Cryptographic Protection	P1	x	x	x	x	2015
SC-15	Collaborative Computing Devices	P1	x	x	x		2016
SC-16	Transmission of Security Attributes	P0					2017
SC-17	Public Key Infrastructure Certificates	P1		x	x		2017
SC-18	Mobile Code	P2		x	x		2017
SC-19	Voice Over Internet Protocol	P1			x		TBD

SYSTEM AND COMMUNICATIONS PROTECTION (SC) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	x	x	x		2016
SC-21	Secure Name /Address Resolution Service ((Recursive or Caching Resolver)	P1	x	x	x		2016
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	x	x	x		2016
SC-23	Session Authenticity	P1		x	x		2017
SC-24	Fail in Known State	P1					2017
SC-25	Thin Nodes	P0					TBD
SC-26	Honeypots	P0					TBD
SC-27	Platform-Independent Applications	P0					TBD
SC-28	Protection of Information at Rest	P1		x	x	x	2015
SC-29	Heterogeneity	P0					TBD
SC-30	Concealment and Misdirection	P0					TBD
SC-31	Covert Channel Analysis	P0					TBD
SC-32	Information System Partitioning	P0					2017
SC-34	Non-Modifiable Executable Programs	P0					2017
SC-35	Honeyclients	P0					TBD
SC-36	Distributed Processing and Storage	P0					TBD
SC-37	Out-of-Band Channels	P0					2017
SC-38	Operations Security	P0					TBD
SC-39	Process Isolation	P1	x	x	x		2016
SC-40	Wireless Link Protection	P0					2017
SC-41	Port and I/O Device Access	P0					TBD
SC-42	Sensor Capability and Data	P0					TBD
SC-43	Usage Restrictions	P0					TBD
SC-44	Detonation Chambers	P0					TBD

SYSTEM AND INFORMATION INTEGRITY(SI) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
SI-1	System and Information Integrity Policy and Procedures	P1	x	x	x		2016
SI-2	Flaw Remediation	P1	x	x	x	x	2015
SI-2(2)	Flaw Remediation (Automated Flaw Remediation Status)	P1			x		2015
SI-3	Malicious Code Protection	P1	x	x	x	x	2015
SI-3(1)	Malicious Code Protection (Central Management)	P1			x		2015
SI-3(2)	Malicious Code Protection (Automatic Updates)	P1			x		2015
SI-4	Information System Monitoring	P1	x	x	x		2015
SI-4(2)	Information System Monitoring (Automated Tools For Real-Time Analysis)	P1			x		2015
SI-4(4)	Information System Monitoring (Inbound and Outbound Communications Traffic)	P1			x		2015
SI-4(5)	Information System Monitoring (System-Generated Alerts)	P1			x		2015
SI-5	Security Alerts, Advisories, and Directives	P1	x	x	x	x	2015
SI-6	Security Function Verification	P1					2017
SI-7	Software, Firmware, and Information Integrity	P1			x		2017
SI-7(1)	Software, Firmware, And Information Integrity (Integrity Checks)	P1			x		2017

SYSTEM AND INFORMATION INTEGRITY(SI) CONTROLS							
(NIST SP 800-53 rev4)			HHS Control Baselines				
CNTL NO	CONTROL NAME	PRIORITY	LOW (Public)	MOD (Agency Sensitive)	HIGH (Confidential Information)	SPI (Standalone/Small Workforce)	Compliance by Date (Calender Year)
SI-7(7)	Software, Firmware, And Information Integrity (Integration Of Detection And Response)	P1			x		2017
SI-8	Spam Protection	P2		x	x		2017
SI-8(1)	Spam Protection (Central Management)	P2			x		2017
SI-8(2)	Spam Protection (Automatic Updates)	P2			x		2017
SI-10	Information Input Validation	P1		x	x		2017
SI-11	Error Handling	P2		x	x		2017
SI-12	Information Handling and Retention	P2	x	x	x		2017
SI-13	Predictable Failure Prevention	P0					TBD
SI-14	Non-Persistence	P0					TBD
SI-15	Information Output Filtering	P0					2017
SI-16	Memory Protection	P1		x	x		2017
SI-17	Fail-Safe Procedures	P0					TBD