



# IT Security Handbook

Security Assessment and Authorization: -  
Continuous Monitoring – Annual Security Control  
Assessments -

Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments

Distribution:

NODIS

Approved



Marion Meissner  
Deputy Chief Information Officer for  
Information Technology Security (Acting)

11/10/2010  
Date

Change History

Version	Date	Change Description
1.0	04/23/10	Initial Draft
2.0	10/05/10	Update name, number, and format. Added Applicable documents section and reference to NPR 2810.1. IR modified to read IM. IT replaced with Information System. Added reference to NPR 2810.1. C&A modified to read Security Assessment and Authorization. Document number changed from ITS-SOP-0012 to ITS-HBK-2810.02-04.

ITS Handbook (ITS-HBK-2810.02-04) -  
Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Table of Contents

1.0	Introduction and Background.....	5 -
2.0	Requirements and Recommendations .....	5 -
3.0	Roles and Responsibilities .....	6 -
4.0	Process for Annual Security Control Assessment .....	7 -
Appendix A: Definitions .....		8 -
Appendix B: Acronyms .....		10 -
Appendix C: Annual Security Control Assessment Worksheet (High System) .....		11 -
Appendix D: Annual Security Control Assessment Worksheet (Moderate System) .....		16 -
Appendix E: Annual Security Control Assessment Worksheet (Low System) .....		20 -

## 1.0 Introduction and Background

According to the recommendations of the National Institute of Standards and Technology (NIST), a well-designed and well-managed continuous monitoring program is essential for a dynamic and effective security control assessment and risk determination process that can provide near real-time security status information.

The hallmarks of a robust continuous monitoring program include:

- Information systems which are firmly governed by established configuration management, change control, and security impact assessment processes;
- Ongoing analysis of security impacts reflected consistently throughout the entire system development lifecycle (SDLC);
- A defined strategy for the holistic assessment of security controls (including system-specific, hybrid, and common controls) that addresses the scope, priority, and frequency of those assessments;
- Status reporting to appropriate organizational officials; and
- Authorizing officials with active involvement in the ongoing management of information systems and related security risks.

An effective continuous monitoring program has the ultimate objective of what NIST refers to as “a state of ongoing authorization”. By consistently maintaining sufficient knowledge of the security state of an information system, an authorizing official may make, at any time, a risk-based determination regarding the acceptable operation of a system. Further, an ongoing understanding of a system’s security posture illuminates what steps in the Risk Management Framework may need to be re-executed in order to adequately mitigate additional risks.

The annual assessment of security controls is an important facet of the continuous monitoring process. This handbook is guided by the principles outlined in *NPR 2810.1, Security of Information Technology*. This handbook defines the NASA processes and procedures for the annual assessment of security controls as accorded by *NIST Special Publication 800-53* and *NIST Special Publication 800-37*. Requirements are described across a three-year assessment and authorization lifecycle.

### Applicable Documents

- - *NIST SP 800-37, Guide for Applying the Risks Management Framework to Federal Information Systems*
- - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
- - *NPR 2810.1, Security of Information Technology*

## 2.0 Requirements and Recommendations

- 2.1 - In endorsement of NIST recommendations, all security controls applicable to a system’s security categorization must be assessed within a three-year assessment and authorization lifecycle.
- 2.2 - In support of NASA reporting requirements, annual assessments of security controls for the current fiscal year must be completed no later than September 30<sup>th</sup>.
- 2.3 - Consistent with the requirements of a three-year assessment and authorization lifecycle, controls considered for annual assessment must include:
  - 2.3.1 Agency Common Controls;
  - 2.3.2 Agency Hybrid Controls;
  - 2.3.3 Agency-Selected Controls;

- 2.3.4 Center Common Controls;
- 2.3.5 Site Common Controls;
- 2.3.6 Controls Related to POA&M Findings; and
- 2.3.7 Some appropriate subset of controls not included in 2.3.1 through 2.3.6, above.
  - 2.3.7.1 An effective continuous monitoring program will assist in the selection of control subsets, and by extension help amortize resource expenditures throughout the assessment and authorization lifecycle.
- 2.4 For systems with security categorizations of moderate or high, all security controls must be assessed by an independent party within the three-year assessment and authorization lifecycle.
  - 2.4.1 If an independent party is used to complete annual assessments, a three-year assessment and authorization lifecycle may adhere to the following recommended track:
    - 2.4.1.1 Initial Authorization (Year 0) – All security controls are assessed by an independent party, and an ATO is granted.
    - 2.4.1.2 Year 1 – Security controls requiring annual assessment, security controls related to POA&M findings, and one-half of all other security controls are assessed.
    - 2.4.1.3 Year 2 – Security controls requiring annual assessment, security controls related to POA&M findings, and one-half of all other security controls (exclusive of those controls assessed in Year 1) are assessed.
    - 2.4.1.4 Year 3 – All security controls are assessed by an independent party, and an ATO is granted.
  - 2.4.2 If an independent party is not used to complete annual assessments, a three-year assessment and authorization lifecycle may adhere to the following recommended track:
    - 2.4.2.1 Initial Authorization (Year 0) – All security controls are assessed, and an ATO is granted.
    - 2.4.2.2 Year 1 – Security controls requiring annual assessment, security controls related to POA&M findings, and one-third of all other security controls are assessed.
    - 2.4.2.3 Year 2 – Security controls requiring annual assessment, security controls related to POA&M findings, and one-third of all other security controls (exclusive of those controls assessed in Year 1) are assessed.
    - 2.4.2.4 Year 3 – Security controls requiring annual assessment, security controls related to POA&M findings, and one-third of all other security controls (exclusive of those controls assessed in Year 1 and Year 2) are assessed, and an ATO is granted.

### 3.0 Roles and Responsibilities

*The Senior Agency Information Security Official (SAISO) shall:*

- Ensures the assessment of all Agency Common Controls.
- Ensures the assessment of those portions of Agency Hybrid Controls which belong to the agency.

*The Information System Owner (ISO) shall:*

- Ensures the completion of an annual security control assessment for their system(s).
- Provides the Security Control Assessor with a completed Annual Security Control Assessment Worksheet (Note: Security categorization specific worksheets may be found in Appendices C, D, and E).
- Ensures the creation of POA&M or the acceptance of risk related to any identified security deficiencies or weaknesses.
- Updates the System Security Plan (SSP) with a Security Assessment Report (SAR) and POA&Ms.

*The Security Control Assessor (SCA) shall:*

- Assesses those portions of Agency Hybrid Controls which belong to the center or site.

- Assesses all security controls as identified in an ISO's completed Annual Security Control Assessment Worksheet.
- Documents annual security control assessment results and generate a SAR.
- Reports immediately any significant security deficiencies or weaknesses to the ISO.

## 4.0 Process for Annual Security Control Assessment

- 4.1 - The ISO completes all general information sections of an Annual Security Control Assessment Worksheet appropriate to the security categorization of a system.
- 4.2 - The ISO identifies the Center Common Controls by marking "X" in the "Center Common Controls" column.
- 4.3 - The ISO identifies the Site Common Controls by marking "X" in the "Site Common Controls" column.
- 4.4 - The ISO identifies any controls related to POA&M findings by marking "X" in the "Controls with POA&M Findings" column.
- 4.5 - The ISO identifies the specific subset of security controls to be assessed for the current fiscal year by marking "X" in the "FY [YYYY]" column.
- 4.6 - The SCA completes assessments for all security controls identified by the Annual Security Control Assessment Worksheet.
- 4.7 - The SCA documents all assessment findings and generates a SAR along with a report of any identified security deficiencies or weaknesses.
- 4.8 - The ISO updates the SSP as appropriate.

## Appendix A: Definitions

<b>Authorization to Operate (ATO)</b>	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls. [NIST]
<b>Common Security Control</b>	A security control that is inherited by an information system. See <i>Security Control Inheritance</i> .  Security control that can be applied to one or more NASA information systems and has the following properties: (1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (2) the results from the assessment of the control can be used to support the security assessments and authorizations processes of an agency information system where that control may have been applied.
<b>High-Impact System</b>	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]
<b>Impact</b>	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
<b>Independent Party</b>	When performing annual assessments, an independent party is a representative with no stake in the system being evaluated. This representative need not be an external contractor, or “third party” organization.
<b>Information Security</b>	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]
<b>Information System (Also referred to as IT System)</b>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502]  (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]
<b>Information System Owner</b>	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [NIST]
<b>Information Technology</b>	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C., Sec. 1401]
<b>Information Technology (IT) System</b>	See information system.
<b>Low-Impact System</b>	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]
<b>Moderate-Impact System</b>	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]
<b>Plan of Action and Milestones</b>	A document that identifies tasks needing to be accomplished, resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. [OMB Memorandum 02-01] (NIST)
<b>Plan of Action and Milestones (POA&amp;M) - Programmatic</b>	A <u>Programmatic</u> POA&M is used to document and track the security deficiencies and/or weaknesses in the security controls of an IT system, multiple IT systems, and/or organizational level policies, programs, and assessment and authorization implementation and the documentation and tracking of the mitigation of these deficiencies. These deficiencies are normally identified from audits/investigations by the OIG, Government Accounting Office (GAO) (congressional), or other authorized agency. A programmatic POA&M shall be managed and tracked at the Agency level and with mitigation reports provided to the agency/organization that identified the deficiency.

ITS Handbook (ITS-HBK-2810.02-04) -  
Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

<b>Plan of Action and Milestones (POA&amp;M) - System</b>	A <u>System</u> POA&M is used to document the security deficiencies and/or weaknesses in the security controls of an information system and to track the mitigation of those deficiencies. These deficiencies are normally identified from the system security control assessments, security impact analyses, and continuous monitoring activities. A POA&M shall be prepared/established for every information system that has a deficiency
<b>Risk</b>	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.  Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. [FIPS 200, Adapted]
<b>Risk Analysis</b>	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
<b>Risk Assessment</b>	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system.  Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
<b>Security Categorization</b>	The process of determining the security category for information or an information system. See <i>Security Category</i> .
<b>Security Category</b>	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operation, organizational assets, individuals, other organizations, and the nation. [FIPS 199 Adapted]
<b>Security Controls</b>	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]
<b>Security Control Assessment</b>	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST]
<b>Security Control Inheritance</b>	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See <i>Common Control</i> . [NIST]
<b>System Security Plan</b>	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]

**Appendix B: Acronyms**

<b>ATO</b>	Authorization to Operate
<b>CIO</b>	Chief Information Officer
<b>FIPS</b>	Federal Information Processing Standards
<b>FY</b>	Fiscal Year
<b>HBK</b>	Handbook
<b>ISO</b>	Information System Owner
<b>IT</b>	Information Technology
<b>ITS</b>	Information Technology Security
<b>NIST</b>	National Institute of Standards and Technology
<b>NODIS</b>	NASA Online Directives Information System
<b>NSAAR</b>	NASA Security Assessment and Authorization Repository
<b>POA&amp;M</b>	Plan of Action and Milestone
<b>SAISO</b>	Senior Agency Information Security Officer
<b>SAR</b>	Security Assessment Report
<b>SCA</b>	Security Control Assessor
<b>SP</b>	Special Publication
<b>SSP</b>	System Security Plan

## Appendix C: Annual Security Control Assessment Worksheet (High System)

<b>Annual Security Control Assessment Worksheet</b>
<b>Information System Name:</b>
<b>Abbreviation:</b>
<b>System Security Plan (SSP) Number:</b>
<b>FIPS 199 System Security Impact Category: HIGH</b>
<b>Information System Owner (ISO):</b>
<b>Annual Security Control Assessment for FY: [YYYY]</b>

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
AC-1	X					
AC-2						
AC-3						
AC-4						
AC-5						
AC-6						
AC-7						
AC-8						
AC-10						
AC-11						
AC-14						
AC-17						
AC-18	(H)-X					
AC-19	(H)-X					
AC-20	(H)-X					
AC-22						
AT-1	X					
AT-2	X					
AT-3						
AT-4	X					
AU-1	X					
AU-2	(H)-X					
AU-3						
AU-4						
AU-5						
AU-6						
AU-7						
AU-8						
AU-9						
AU-10						
AU-11						
AU-12						
CA-1	X					

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
CA-2						
CA-3						
CA-5		X				
CA-6						
CA-7						
CM-1	X					
CM-2		X				
CM-3		X				
CM-4		X				
CM-5		X				
CM-6	(H)-X					
CM-7		X				
CM-8		X				
CM-9	X					
CP-1	X					
CP-2		X				
CP-3		X				
CP-4		X				
CP-5						
CP-6		X				
CP-7		X				
CP-8	X					
CP-9		X				
CP-10		X				
IA-1	X					
IA-2						
IA-3						
IA-4						
IA-5						
IA-6						
IA-7						
IA-8						
IM-1	X					
IM-2	(H)-X					
IM-3	(H)-X					
IM-4	(H)-X					
IM-5	X					
IM-6	(H)-X					
IM-7	X					
IM-8	X					
MA-1	(H)-X					
MA-2						
MA-3						

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
MA-4						
MA-5						
MA-6						
MP-1	X					
MP-2						
MP-3						
MP-4						
MP-5						
MP-6						
PE-1	X					
PE-2						
PE-3						
PE-4						
PE-5						
PE-6						
PE-7						
PE-8						
PE-9						
PE-10						
PE-11						
PE-12						
PE-13						
PE-14						
PE-15						
PE-16						
PE-17						
PE-18						
PL-1	X					
PL-2						
PL-4	(H)-X					
PL-5						
PL-6						
PS-1	X					
PS-2						
PS-3						
PS-4						
PS-5						
PS-6						
PS-7	(H)-X					
PS-8						
RA-1	X					
RA-2						
RA-3						

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
RA-5						
SA-1	X					
SA-2						
SA-3						
SA-4	X					
SA-5						
SA-6						
SA-7						
SA-8						
SA-9						
SA-10						
SA-11						
SA-12						
SA-13						
SC-1	X					
SC-2						
SC-3						
SC-4						
SC-5						
SC-7						
SC-8						
SC-9						
SC-10						
SC-12	(H)-X					
SC-13						
SC-14						
SC-15						
SC-17	X					
SC-18	(H)-X					
SC-19	(H)-X					
SC-20						
SC-21						
SC-22						
SC-23						
SC-24						
SC-28						
SC-32						
SI-1	X					
SI-2						
SI-3						
SI-4	(H)-X					
SI-5	(H)-X					
SI-6						

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
SI-7						
SI-8	(H)-X					
SI-9						
SI-10						
SI-11						
SI-12						

## Appendix D: Annual Security Control Assessment Worksheet (Moderate System)

Annual Security Control Assessment Worksheet						
Information System Name:						
Abbreviation:						
System Security Plan (SSP) Number:						
FIPS 199 System Security Impact Category: Moderate						
Information System Owner (ISO):						
Annual Security Control Assessment for FY: [YYYY]						

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
AC-1	X					
AC-2						
AC-3						
AC-4						
AC-5						
AC-6						
AC-7						
AC-8						
AC-11						
AC-14						
AC-17						
AC-18	(H)-X					
AC-19	(H)-X					
AC-20	(H)-X					
AC-22						
AT-1	X					
AT-2	X					
AT-3						
AT-4	X					
AU-1	X					
AU-2	(H)-X					
AU-3						
AU-4						
AU-5						
AU-6						
AU-7						
AU-8						
AU-9						
AU-11						
AU-12						
CA-1	X					
CA-2						
CA-3						

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
CA-5		X				
CA-6						
CA-7						
CM-1	X					
CM-2		X				
CM-3		X				
CM-4		X				
CM-5		X				
CM-6	(H)-X					
CM-7		X				
CM-8		X				
CM-9	X					
CP-1	X					
CP-2		X				
CP-3		X				
CP-4		X				
CP-5						
CP-6		X				
CP-7		X				
CP-8	X					
CP-9		X				
CP-10		X				
IA-1	X					
IA-2						
IA-3						
IA-4						
IA-5						
IA-6						
IA-7						
IA-8						
IM-1	X					
IM-2	(H)-X					
IM-3	(H)-X					
IM-4	(H)-X					
IM-5	X					
IM-6	(H)-X					
IM-7	X					
IM-8	X					
MA-1	(H)-X					
MA-2						
MA-3						
MA-4						
MA-5						

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
MA-6						
MP-1	X					
MP-2						
MP-3						
MP-4						
MP-5						
MP-6						
PE-1	X					
PE-2						
PE-3						
PE-4						
PE-5						
PE-6						
PE-7						
PE-8						
PE-9						
PE-10						
PE-11						
PE-12						
PE-13						
PE-14						
PE-15						
PE-16						
PE-17						
PE-18						
PL-1	X					
PL-2						
PL-4	(H)-X					
PL-5						
PL-6						
PS-1	X					
PS-2						
PS-3						
PS-4						
PS-5						
PS-6						
PS-7	(H)-X					
PS-8						
RA-1	X					
RA-2						
RA-3						
RA-5						
SA-1	X					

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
SA-2						
SA-3						
SA-4	X					
SA-5						
SA-6						
SA-7						
SA-8						
SA-9						
SA-10						
SA-11						
SC-1	X					
SC-2						
SC-4						
SC-5						
SC-7						
SC-8						
SC-9						
SC-10						
SC-12	(H)-X					
SC-13						
SC-14						
SC-15						
SC-17	X					
SC-18	(H)-X					
SC-19	(H)-X					
SC-20						
SC-22						
SC-23						
SC-28						
SC-32						
SI-1	X					
SI-2						
SI-3						
SI-4	(H)-X					
SI-5	(H)-X					
SI-7						
SI-8	(H)-X					
SI-9						
SI-10						
SI-11						
SI-12						

## Appendix E: Annual Security Control Assessment Worksheet (Low System)

<b>Annual Security Control Assessment Worksheet</b>
<b>Information System Name:</b>
<b>Abbreviation:</b>
<b>System Security Plan (SSP) Number:</b>
<b>FIPS 199 System Security Impact Category: Low</b>
<b>Information System Owner (ISO):</b>
<b>Annual Security Control Assessment for FY: [YYYY]</b>

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
AC-1	X					
AC-2						
AC-3						
AC-7						
AC-8						
AC-14						
AC-17						
AC-18	(H)-X					
AC-19	(H)-X					
AC-20	(H)-X					
AC-22						
AT-1	X					
AT-2	X					
AT-3						
AT-4	X					
AU-1	X					
AU-2	(H)-X					
AU-3						
AU-4						
AU-5						
AU-6						
AU-8						
AU-9						
AU-11						
AU-12						
CA-1	X					
CA-2		X				
CA-3						
CA-5		X				
CA-6						
CA-7		X				
CM-1	X					
CM-2		X				

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
CM-4		X				
CM-6	(H)-X					
CM-7		X				
CM-8		X				
CP-1	X					
CP-2		X				
CP-3		X				
CP-4		X				
CP-9		X				
CP-10		X				
IA-1	X					
IA-2						
IA-4						
IA-5						
IA-6						
IA-7						
IA-8						
IM-1	X					
IM-2	(H)-X					
IM-4	(H)-X					
IM-5	X					
IM-6	(H)-X					
IM-7	X					
IM-8	X					
MA-1	(H)-X					
MA-2						
MA-4						
MA-5						
MP-1	X					
MP-2						
MP-6						
PE-1	X					
PE-2						
PE-3						
PE-6						
PE-7						
PE-8						
PE-12						
PE-13						
PE-14						
PE-15						
PE-16						
PL-1	X					

ITS Handbook (ITS-HBK-2810.02-04) -  
 Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments -

Control Number	Agency Common Controls [H = Hybrid]	Agency Selected Controls	Center Common Controls	Site Common Controls	Controls with POA&M Findings	FY [YYYY] Controls
PL-2						
PL-4	(H)-X					
PL-5						
PS-1	X					
PS-2						
PS-3						
PS-4						
PS-5						
PS-6						
PS-7	(H)-X					
PS-8						
RA-1	X					
RA-2						
RA-3						
RA-5						
SA-1	X					
SA-2						
SA-3						
SA-4	X					
SA-5						
SA-6						
SA-7						
SA-9						
SC-1	X					
SC-5						
SC-7						
SC-12	(H)-X					
SC-13						
SC-14						
SC-15						
SC-20						
SI-1	X					
SI-2						
SI-3						
SI-5	(H)-X					
SI-12						