



OFFICE OF THE SECRETARY OF DEFENSE  
1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000

APR 21 2016

MEMORANDUM FOR ASSISTANT SECRETARIES OF THE MILITARY DEPARTMENTS  
(FINANCIAL MANAGEMENT AND COMPTROLLER)  
CHIEF INFORMATION OFFICERS OF THE MILITARY  
DEPARTMENTS  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES  
COMPTROLLER, JOINT STAFF  
CHIEF FINANCIAL OFFICER/COMPTROLLER, U.S. SPECIAL  
OPERATIONS COMMAND  
CHIEF INFORMATION OFFICER, U.S. SPECIAL OPERATIONS  
COMMAND  
DIRECTOR, PROGRAM ANALYSIS AND FINANCIAL  
MANAGEMENT, U.S. TRANSPORTATION COMMAND  
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND  
CYBER SYSTEMS, U.S. TRANSPORTATION COMMAND

SUBJECT: Enhanced Integration of Financial Management Requirements with the Risk  
Management Framework


The National Defense Authorization Act for Fiscal Year (FY) 2010, section 1003, requires the Department to validate its financial statements are audit-ready not later than September 30, 2017. Although much has been accomplished, focused attention needs to be placed on additional practices and security controls over information systems that impact financial reporting.

In support of the DoD FY 2014 Information Resources Management Strategic Management Plan, the Department of Defense Chief Information Officer (DoD CIO) updated DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," to facilitate meeting the Financial Improvement and Audit Readiness (FIAR) requirements for relevant systems. Additionally, the Office of the Under Secretary of Defense (Comptroller) (OUSDC), in collaboration with the DoD CIO, developed the attached guidance to incorporate FIAR requirements into the RMF process. By following the guidance, the Department will more efficiently and consistently meet the RMF and Federal Information System Controls Audit Manual financial audit expectations. This guidance should be followed for financial management system authorizations performed under the RMF or its predecessor, the DoD Information Assurance Certification and Accreditation Process (DIACAP).


As the Department transitions from DIACAP to RMF, there may be cases where systems that have an authority to operate under DIACAP may impact your financial statement audit or examination. In these cases, additional procedures to fully address the FIAR Guidance requirements must be completed prior to the beginning of FY 2018.



The OUSD(C) and DoD CIO will continue to review existing policy and procedures and incorporate additional FIAR requirements as needed. The points of contact are Ms. Mobola Kadiri, OUSD(C), 571-256-2670, mobola.a.kadiri.civ@mail.mil; and Ms. Lindy Burkhardt, DoD CIO, 703-614-1996, linderman.l.burkhart.civ@mail.mil.



Richard A. Hale  
Deputy Chief Information Officer  
for Cybersecurity  
Office of the DoD Chief Information Officer



Mark E. Easton  
Deputy Chief Financial Officer  
Office of the Under Secretary of Defense  
(Comptroller)

Attachment:  
As stated

cc:  
Principal Deputy Under Secretaries of Defense  
Assistant Deputy Chief Management Officer  
Deputy Inspector General for Auditing, DoD Office of Inspector General

# **Enhanced Integration of Financial Management Requirements with the Risk Management Framework**

## **Purpose**

The objective of a financial statement audit is to obtain an opinion on whether an organization's financial statements have been prepared in accordance with generally accepted accounting principals. To render these opinions, independent auditors perform tests of system controls, business process controls, and tests of substantive account details in accordance with generally accepted auditing standards.

The DoD Instruction 8510.01 "Risk Management Framework (RMF) for DoD Information Technology" system assessment and authorization requirements were not developed to meet system audit readiness requirements as defined in the Department's Financial Improvement and Audit Readiness (FIAR) Guidance or system internal control requirements defined in OMB Circular A-123 Appendix A. For example:

- The RMF allows for documenting the goal of an internal controls versus identifying and documenting the actual control procedure in place.
- The RMF allows for testing of the most recent three to five occurrences of an activity versus testing larger sample sizes from a longer historical period of time.
- The RMF may allow acceptance of risks that would not be accepted by an independent financial statement auditor.

This Guidance provides instructions to assist those completing the system assessment and authorization process (for systems that impact internal controls over financial reporting) to concurrently address controls that will impact the financial statement audit readiness of these systems. For those systems that have previously obtained an authority to operate under either DoD Information Assurance Certification and Accreditation Process (DIACAP) or RMF, the organization will need to perform additional procedures where necessary to fully address the FIAR Guidance requirements.

This Guidance is presented in the format of an RMF overlay with additional appendices that provide the following:

- Appendix 1 - Summary of FIAR Guidance requirements relating to the system and associated infrastructure components to be included in the scope of the assessment, defining control objectives, documentation of controls, testing of controls, and evaluation of results.
- Appendix 2 - A detailed mapping of Federal Information System Controls Audit Manual (FISCAM) control techniques to National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST 800-53)
- NIST 800-53 security controls to assist in the identification of common audit readiness and assessment and authorization requirements.

## Identification

The Guidance for systems impacting DoD financial statement audits defines requirements for systems affecting Department of Defense (DoD) financial reporting and audit readiness. The following public laws, regulations, DoD policies, and instructions define additional requirements:

- The Chief Financial Officers Act of 1990 (CFO Act), as amended (P.L. 101–576, as codified in 31 USC 3512), November 1990
- National Defense Authorization Act of 2013 (H.R. 4310), January 2012
- National Defense Authorization Act of 2011 (H.R. 6523), January 2011
- National Defense Authorization Act of 2010 (P.L. 111–84), October 2009
- The Federal Managers' Financial Integrity Act of 1982 (FMFIA), as amended (P.L. 97-255, as codified in 31 USC 3512), September 1982
- The Federal Financial Management Improvement Act of 1996 (FFMIA), as amended (P.L. 104-208, as codified in 31 USC 3512), September 1996
- The Office of Management and Budget (OMB) Circular No. A-123, Management's Responsibility for Internal Control, December 2004
- The OMB Circular No. A-130, Management of Federal Information Resources, November 2000
- The E-Government Act (includes the Federal Information Security Management Act, P.L. 107-347), December 2002

The Guidance is based on the following:

- United States Government Accountability Office (GAO), Federal Information System Controls Audit Manual (FISCAM), (GAO-09-232G), February 2009
- GAO, Standards for Internal Control in the Federal Government, (GAO-14-704G), September 2014.
- GAO and the President's Council on Integrity and Efficiency (PCIE), (GAO-08-585G), Financial Audit Manual (FAM), July 2008
- National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 2014 (NIST SP 800-53)
- CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems, March 15, 2012
- Financial Improvement and Audit Readiness (FIAR) Guidance, April 2015
- DoDI 5010.40, Manager's Internal Control Program (MICP) Procedures, May 2013

### 1. Guidance Characteristics

This Guidance applies to systems that record accounting events relevant to DoD financial management, impact the Department's internal controls over financial reporting (ICOFR), or affect the auditability of the Department's financial statements.

**Internal Control** - Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved (see fig. 2). These objectives and related risks can be broadly classified into one or more of the following three categories:

- **Operations** - Effectiveness and efficiency of operations
- **Reporting** - Reliability of reporting for internal and external use
- **Compliance** - Compliance with applicable laws and regulations

*Figure 1 - Internal Control as defined in GAO-14-704G  
(Standards for Internal Control in the Federal Government)*

To ensure the audit readiness of these systems, additional requirements beyond those defined by DoD and Committee on National Security Systems (CNSS) policies are documented in the remainder of this Guidance. Additional requirements, defined in Risk Management Framework Overlays may also be applied to address specialized needs (e.g., personally identifiable information, systems operating within a tactical environment).

Systems subject to this Guidance must satisfy the requirements defined in the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)), *Financial Improvement and Audit Readiness (FIAR) Guidance*<sup>1</sup>, Department of Defense Instruction (DoDI) 5010.40, *Managers' Internal Control Program Procedures*<sup>2</sup>, and related laws, regulations, instructions, directives, and policies. The specific set of compliance requirements that must be satisfied, for each system, will be based on an analysis of each system's function in the processing of DoD financial events, ICOFR, and financial statement audit.

## **2. Applicability**

This Guidance for systems impacting DoD financial statement audits is intended to assist in identifying the systems subject to the FIAR Guidance and other requirements. This Instruction also provides guidance regarding the appropriate documentation and testing of Information Technology (IT) General and Application controls to achieve and sustain audit readiness and to ensure internal controls over financial reporting comply with applicable laws and regulations.

---

<sup>1</sup> [http://comptroller.defense.gov/Portals/45/documents/fiar/fiar\\_guidance.pdf](http://comptroller.defense.gov/Portals/45/documents/fiar/fiar_guidance.pdf)

<sup>2</sup> [http://comptroller.defense.gov/Portals/45/documents/micp\\_docs/introduction/DoDI\\_5010-40\\_May\\_30\\_2013.pdf](http://comptroller.defense.gov/Portals/45/documents/micp_docs/introduction/DoDI_5010-40_May_30_2013.pdf)

IT General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entity-wide, system, and business process application levels.

IT business process application level controls, commonly referred to as application level controls or application controls, are those controls over the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

**Figure 2 - Internal General and Application Control as defined in (GAO-09-232G)  
(Federal Information System Controls Audit Manual)**

Personnel responsible for implementing CNSSI No. 1253 baselines for individual systems should also assess the materiality (relative significance) of the system with regards to financial processes to determine if it should be categorized as a financial management system.

Materiality is the magnitude of an item's omission or misstatement in a financial statement that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item.

**Figure 3 - Materiality as defined in GAO-08-585G  
(Financial Audit Manual)**

The information system owner and security officials identifying the appropriate security controls for the system must collaborate with the finance or program management office to determine if the system impacts the organization's financial management processes and internal controls over financial reporting.

The following initial questions should be answered to determine if the system impacts the financial statements

- 1) Does the information system perform any activity having financial consequences to the Federal government (i.e., perform a ***financial/accounting event***)?
- 2) Does the system process transactions or store information that directly or indirectly triggers a ***financial event*** (see definitions section)?
- 3) Does the system collect, process, maintain, transmit, or report data regarding events that impact financial reporting?

**Figure 4 - Initial questions for determining if a system performs functions that impact financial management. (OMB Circular A-127)**

If the answer to any of the above questions is yes, the following criteria should be applied to determine if there is any impact to the organization's internal controls over financial reporting.

- 1) Controls within the system are identified as key controls in the internal controls assessment (ex., automated edit checking);
- 2) Systems are used to generate or store original key supporting documentation;
- 3) Reports generated by the system are utilized in the execution of key controls; or
- 4) Systems are relied upon to perform material calculations (e.g., to compute payroll).
- 5) Has the business process owner concurred the system impacts internal control over financial reporting and must be relied upon for audit readiness.

***Figure 5 - Criteria for determining if a system impacts internal controls over financial reporting. (FIAR Guidance)***

If any of the criteria above are applicable to a system and the organization has not identified, documented, and tested mitigating controls sufficient to eliminate the identified reliance on the system, then the guidance in this document must be applied for the system. Furthermore, the finance or program management office (responsible for financial statement audit readiness) must approve the assessment and authorization results for these systems.

### **3. Summarized Guidance Control Specifications**

Table 1 is based on FISCAM Appendix IV, Mapping FISCAM to NIST SP 800-53 and Other Related NIST Publications.

- A plus sign (+) indicates the Risk Management Framework security control should be selected if the associated FISCAM control technique is deemed necessary to satisfy one or more control objectives.\*
- The letter E indicates there is a control extension.
- The letter G indicates there is guidance, including specific tailoring guidance, if applicable, for the control.
- The letter V indicates this Guidance defines a value for an organizationally-defined parameter for the control.
- The letter R indicates there is at least one regulatory or statutory reference that requires or prohibits the control selection or that the control helps to meet the regulatory or statutory requirements.

\* Due to the varying levels of system functionality and audit relevance, vast differences in technical complexity and architecture, and options for managing information systems, the GAO FISCAM does not provide a pre-defined number or sub-set of the control techniques that must be addressed for all systems. Rather, the FISCAM and FIAR methodologies focus on identifying, documenting, and testing controls necessary to satisfy the in-scope control objectives for each system environment. However, the *DoD IG and GAO approved FIAR Guidance* identifies a subset of FISCAM control techniques that are most likely to be relevant to financial statement

audit readiness and should be considered as a higher priority. References to these higher priority FISCAM control techniques will appear in **bold** text throughout this document. The remaining FISCAM control techniques should be reviewed to determine whether there are unique circumstances for an individual system that would cause them to also be relevant to financial statement audit readiness.

As it is not possible to pre-determine the population of FISCAM control techniques relevant for every system, Table 1 was developed assuming all FISCAM control techniques may be in-scope and identifies the associated RMF/NIST security controls. If during the audit readiness process it is determined that a FISCAM control technique is not key to addressing the control objectives, then the associated RMF/NIST security control would no longer be required for financial statement audit readiness purposes.



**Table 1: Guidance Security Controls**

Row	Control	Guidance	Control	Guidance	Control	Guidance
1	AC-1	+	AC-2	V+	AC-2 (1)	+
2	AC-2 (2)	+	AC-2 (3)	+	AC-2 (4)	+
3	AC-2 (5)	G+	AC-2 (7)	+	AC-2 (9)	+
4	AC-2 (10)	+	AC-2 (11)	+	AC-2 (12)	+
5	AC-2 (13)	+	AC-3	+	AC-3 (2)	+
6	AC-3 (3)	+	AC-3 (4)	+	AC-3 (5)	+
7	AC-3 (7)	+	AC-3 (8)	+	AC-3 (9)	+
8	AC-3 (10)	+	AC-4	+	AC-4 (1)	+
9	AC-4 (2)	+	AC-4 (3)	+	AC-4 (7)	+
10	AC-4 (8)	+	AC-4 (9)	+	AC-4 (10)	+
11	AC-4 (11)	+	AC-4 (12)	+	AC-4 (17)	+
12	AC-4 (20)	+	AC-4 (21)	+	AC-4 (22)	+
13	AC-5	+	AC-6	+	AC-6 (1)	+
14	AC-6 (2)	+	AC-6 (3)	+	AC-6 (4)	+
15	AC-6 (5)	+	AC-6 (6)	+	AC-6 (7)	+
16	AC-6 (9)	+	AC-6 (10)	+	AC-7	+
17	AC-8	+	AC-9	+	AC-9 (1)	+
18	AC-10	+	AC-11	+	AC-11 (1)	G+
19	AC-12	+	AC-12 (1)	+	AC-14	+
20	AC-16	+	AC-16 (1)	+	AC-16 (2)	+
21	AC-16 (3)	+	AC-16 (4)	+	AC-16 (10)	+
22	AC-17	+	AC-17 (1)	+	AC-17 (2)	+
23	AC-17 (3)	+	AC-17 (4)	+	AC-17 (6)	+
24	AC-18	+	AC-18 (1)	+	AC-18 (3)	+
25	AC-18 (4)	+	AC-18 (5)	+	AC-19	+
26	AC-19 (5)	+	AC-20	+	AC-20 (1)	+
27	AC-20 (2)	+	AC-20 (3)	+	AC-20 (4)	+
28	AC-21	+	AC-22	+	AC-23	+
29	AC-24	+	AC-24 (1)	+	AC-25	+
30	AT-1	+	AT-2	+	AT-2 (1)	+
31	AT-2 (2)	+	AT-3	+	AT-3 (1)	+
32	AT-3 (2)	+	AT-3 (3)	+	AT-3 (4)	+
33	AT-4	+	AU-1	+	AU-2	+
34	AU-2 (3)	+	AU-3	+	AU-4	+
35	AU-4 (1)	+	AU-5	+	AU-5 (1)	+
36	AU-5 (2)	+	AU-6	+	AU-6 (1)	+
37	AU-6 (7)	+	AU-6 (10)	+	AU-7	+

Row	Control	Guidance	Control	Guidance	Control	Guidance
38	AU-7 (1)	+	AU-8	+	AU-8 (1)	+
39	AU-9	+	AU-9 (2)	+	AU-9 (4)	+
40	AU-9 (6)	+	AU-10	+	AU-10 (1)	+
41	AU-10 (2)	+	AU-10 (3)	+	AU-10 (4)	+
42	AU-11	+	AU-12	+	AU-12 (3)	+
43	CA-1	+	CA-2	+	CA-2 (1)	+
44	CA-2 (2)	+	CA-2 (3)	+	CA-3	+
45	CA-3 (1)	+	CA-3 (3)	+	CA-3 (4)	+
46	CA-3 (5)	+	CA-5	+	CA-6	+
47	CA-7	+	CA-7 (1)	+	CA-8	+
48	CA-8 (1)	+	CA-9	+	CA-9 (1)	+
49	CM-1	+	CM-2	+	CM-2 (1)	+
50	CM-3	+	CM-3 (2)	+	CM-3 (4)	+
51	CM-3 (6)	+	CM-4	+	CM-4 (1)	+
52	CM-4 (2)	+	CM-5	+	CM-5 (1)	+
53	CM-5 (2)	+	CM-5 (4)	+	CM-5 (5)	+
54	CM-5 (6)	+	CM-6	+	CM-6 (1)	+
55	CM-6 (2)	+	CM-7	+	CM-7 (1)	+
56	CM-7 (2)	+	CM-7 (3)	+	CM-8	+
57	CM-8 (1)	+	CM-8 (2)	+	CM-8-3	+
58	CM-8 (4)	+	CM-8 (5)	+	CM-8 (6)	+
59	CM-8 (7)	+	CM-8 (9)	+	CM-9	+
60	CM-9 (1)	+	CM-10	+	CM-11	+
61	CM-11 (1)	+	CM-11 (2)	+	CP-1	+
62	CP-2	+	CP-2 (1)	+	CP-2 (2)	+
63	CP-2 (3)	+	CP-2 (4)	+	CP-2 (5)	+
64	CP-2 (6)	+	CP-2 (7)	+	CP-2 (8)	+
65	CP-3	+	CP-3 (1)	+	CP-3 (2)	+
66	CP-4	+	CP-4 (1)	+	CP-4 (2)	+
67	CP-4 (3)	+	CP-4 (4)	+	CP-6	+
68	CP-6 (1)	+	CP-6 (2)	+	CP-6 (3)	+
69	CP-7	+	CP-7 (1)	+	CP-7 (2)	+
70	CP-7 (3)	+	CP-7 (4)	+	CP-7 (6)	+
71	CP-8	+	CP-8 (1)	+	CP-8 (2)	+
72	CP-8 (3)	+	CP-8 (4)	+	CP-8 (5)	+
73	CP-9	+	CP-9 (1)	+	CP-9 (2)	+
74	CP-9 (3)	+	CP-9 (5)	+	CP-9 (6)	+
75	CP-10	+	CP-10 (2)	+	CP-10 (4)	+
76	CP-10 (6)	+	IA-1	+	IA-2	+
77	IA-2 (1)	+	IA-2 (2)	+	IA-2 (3)	+

Row	Control	Guidance	Control	Guidance	Control	Guidance
78	IA-2 (4)	+	IA-2 (5)	+	IA-2 (6)	+
79	IA-2 (7)	+	IA-2 (8)	+	IA-2 (9)	+
80	IA-2 (10)	+	IA-2 (11)	+	IA-2 (12)	+
81	IA-2 (13)	+	IA-3	+	IA-3 (1)	+
82	IA-3 (3)	+	IA-3 (4)	+	IA-4	+
83	IA-4 (1)	+	IA-4 (2)	+	IA-4 (3)	+
84	IA-4 (4)	+	IA-4 (5)	+	IA-4 (6)	+
85	IA-4 (7)	+	IA-5	+	IA-5 (1)	+
86	IA-5 (2)	+	IA-5 (3)	+	IA-5 (4)	+
87	IA-5 (5)	+	IA-5 (6)	+	IA-5 (7)	+
88	IA-5 (8)	+	IA-5 (9)	+	IA-5 (10)	+
89	IA-5 (11)	+	IA-5 (12)	+	IA-5 (13)	+
90	IA-5 (14)	+	IA-5 (15)	+	IA-6	+
91	IA-7	+	IA-8	+	IA-8 (1)	+
92	IA-8 (2)	+	IA-8 (3)	+	IA-8 (4)	+
93	IA-8 (5)	+	IA-9	+	IA-9 (1)	+
94	IA-9 (2)	+	IA-10	+	IR-1	+
95	IR-2	+	IR-2 (1)	+	IR-3	+
96	IR-3 (2)	+	IR-4	+	IR-4 (1)	+
97	IR-4 (2)	+	IR-4 (3)	+	IR-4 (4)	+
98	IR-4 (5)	+	IR-4 (6)	+	IR-4 (7)	+
99	IR-4 (8)	+	IR-4 (9)	+	IR-4 (10)	+
100	IR-5	+	IR-5 (1)	+	IR-6	+
101	IR-6 (1)	+	IR-6 (2)	+	IR-6 (3)	+
102	IR-7	+	IR-7 (2)	+	IR-8	+
103	IR-9	+	IR-9 (1)	+	IR-9 (2)	+
104	IR-9 (3)	+	IR-9 (4)	+	IR-10	+
105	MA-1	+	MA-2	+	MA-2 (2)	+
106	MA-4	+	MA-4 (1)	+	MA-4 (2)	+
107	MA-4 (3)	+	MA-4 (4)	+	MA-4 (5)	+
108	MA-4 (6)	+	MA-4 (7)	+	MA-6	+
109	MA-6 (1)	+	MA-6 (2)	+	MA-6 (3)	+
110	MP-1	+	MP-2	+	MP-3	+
111	MP-4	+	MP-4 (2)	+	MP-5	+
112	MP-5 (3)	+	MP-5 (4)	+	MP-6	+
113	MP-6 (1)	+	MP-6 (2)	+	MP-6 (3)	+
114	MP-6 (7)	+	MP-6 (8)	+	MP-7	+
115	MP-7 (1)	+	MP-7 (2)	+	MP-8	+
116	MP-8 (1)	+	MP-8 (2)	+	MP-8 (3)	+
117	MP-8 (4)	+	PE-1	+	PE-2	+

Row	Control	Guidance	Control	Guidance	Control	Guidance
118	PE-2 (1)	+	PE-2 (2)	+	PE-2 (3)	+
119	PE-3	+	PE-3 (1)	+	PE-3 (2)	+
120	PE-3 (3)	+	PE-3 (4)	+	PE-3 (5)	+
121	PE-3 (6)	+	PE-4	+	PE-5	+
122	PE-5 (1)	+	PE-5 (2)	+	PE-5 (3)	+
123	PE-6	+	PE-6 (1)	+	PE-6 (2)	+
124	PE-6 (3)	+	PE-6 (4)	+	PE-8	+
125	PE-8 (1)	+	PE-9	+	PE-9 (1)	+
126	PE-9 (2)	+	PE-10	+	PE-11	+
127	PE-11 (1)	+	PE-11 (2)	+	PE-12	+
128	PE-12 (1)	+	PE-13	+	PE-13 (1)	+
129	PE-13 (2)	+	PE-13 (3)	+	PE-13 (4)	+
130	PE-14	+	PE-14 (1)	+	PE-14 (2)	+
131	PE-15	+	PE-15 (1)	+	PE-16	+
132	PE-17	+	PE-18	+	PE-18 (1)	+
133	PL-1	+	PL-2	+	PL-2 (3)	+
134	PL-4	+	PL-4 (1)	+	PL-7	+
135	PS-1	+	PS-2	+	PS-3	+
136	PS-3 (1)	+	PS-3 (2)	+	PS-3 (3)	+
137	PS-4	+	PS-4 (1)	+	PS-4 (2)	+
138	PS-5	+	PS-6	+	PS-6 (2)	+
139	PS-6 (3)	+	PS-7	+	PS-8	+
140	RA-1	+	RA-2	+	RA-3	+
141	RA-5	+	RA-5 (1)	+	RA-5 (2)	+
142	RA-5 (3)	+	RA-5 (4)	+	RA-5 (5)	+
143	RA-5 (6)	+	RA-5 (8)	+	RA-5 (10)	+
144	RA-6	+	SA-1	+	SA-2	+
145	SA-3	+	SA-4	+	SA-4 (1)	+
146	SA-4 (2)	+	SA-4 (3)	+	SA-4 (5)	+
147	SA-4 (6)	+	SA-4 (7)	+	SA-4 (8)	+
148	SA-4 (9)	+	SA-4 (10)	+	SA-5	+
149	SA-8	+	SA-9	+	SA-9 (1)	+
150	SA-9 (2)	+	SA-9 (3)	+	SA-9 (4)	+
151	SA-9 (5)	+	SA-10	+	SA-10 (1)	+
152	SA-10 (2)	+	SA-10 (3)	+	SA-10 (4)	+
153	SA-10 (5)	+	SA-10 (6)	+	SA-11	+
154	SA-11 (1)	+	SA-11 (2)	+	SA-11 (3)	+
155	SA-11 (4)	+	SA-11 (5)	+	SA-11 (6)	+
156	SA-11 (7)	+	SA-11 (8)	+	SA-12	+
157	SA-12 (1)	+	SA-12 (2)	+	SA-12 (5)	+

Row	Control	Guidance	Control	Guidance	Control	Guidance
158	SA-12 (7)	+	SA-12 (8)	+	SA-12 (9)	+
159	SA-12 (10)	+	SA-12 (11)	+	SA-12 (12)	+
160	SA-12 (13)	+	SA-12 (14)	+	SA-12 (15)	+
161	SA-13	+	SA-14	+	SA-15	+
162	SA-15 (1)	+	SA-15 (2)	+	SA-15 (3)	+
163	SA-15 (4)	+	SA-15 (5)	+	SA-15 (6)	+
164	SA-15 (7)	+	SA-15 (8)	+	SA-15 (9)	+
165	SA-15 (10)	+	SA-15 (11)	+	SA-16	+
166	SA-17	+	SA-17 (1)	+	SA-17 (2)	+
167	SA-17 (3)	+	SA-17 (4)	+	SA-17 (5)	+
168	SA-17 (6)	+	SA-17 (7)	+	SA-18	+
169	SA-18 (1)	+	SA-18 (2)	+	SA-21	+
170	SA-21 (1)	+	SC-1	+	SC-2	+
171	SC-2 (1)	+	SC-3	+	SC-3 (1)	+
172	SC-3 (2)	+	SC-3 (3)	+	SC-3 (4)	+
173	SC-3 (5)	+	SC-5	+	SC-5 (1)	+
174	SC-5 (2)	+	SC-5 (3)	+	SC-6	+
175	SC-7	+	SC-7 (3)	+	SC-7 (4)	+
176	SC-7 (5)	+	SC-7 (7)	+	SC-7 (8)	+
177	SC-7 (9)	+	SC-7 (10)	+	SC-7 (11)	+
178	SC-7 (12)	+	SC-7 (13)	+	SC-7 (14)	+
179	SC-7 (15)	+	SC-7 (16)	+	SC-7 (17)	+
180	SC-7 (18)	+	SC-7 (19)	+	SC-7 (20)	+
181	SC-7 (21)	+	SC-7 (22)	+	SC-7 (23)	+
182	SC-8	+	SC-8 (1)	+	SC-8 (2)	+
183	SC-8 (3)	+	SC-8 (4)	+	SC-10	+
184	SC-11	+	SC-11 (1)	+	SC-12	+
185	SC-12 (1)	+	SC-12 (2)	+	SC-12 (3)	+
186	SC-13	+	SC-15	+	SC-15 (1)	+
187	SC-15 (2)	+	SC-15 (3)	+	SC-15 (4)	+
188	SC-16	+	SC-16 (1)	+	SC-17	+
189	SC-18	+	SC-18 (1)	+	SC-18 (2)	+
190	SC-18 (3)	+	SC-18 (4)	+	SC-18 (5)	+
191	SC-19	+	SC-20	+	SC-20 (2)	+
192	SC-21	+	SC-22	+	SC-23	+
193	SC-23 (1)	+	SC-23 (3)	+	SC-23 (5)	+
194	SC-28	+	SC-28 (1)	+	SC-28 (2)	+
195	SC-32	+	SC-36	+	SC-36 (1)	+
196	SC-37	+	SC-37 (1)	+	SC-38	+
197	SC-40	+	SC-41	+	SC-43	+

Row	Control	Guidance	Control	Guidance	Control	Guidance
198	SI-1	+	SI-2	+	SI-2 (1)	+
199	SI-2 (2)	+	SI-2 (3)	+	SI-2 (5)	+
200	SI-2 (6)	+	SI-3	+	SI-3 (1)	+
201	SI-3 (2)	+	SI-3 (4)	+	SI-3 (6)	+
202	SI-3 (7)	+	SI-3 (8)	+	SI-3 (9)	+
203	SI-3 (10)	+	SI-4	+	SI-4 (1)	+
204	SI-4 (2)	+	SI-4 (3)	+	SI-4 (4)	+
205	SI-4 (5)	+	SI-4 (7)	+	SI-4 (9)	+
206	SI-4 (10)	+	SI-4 (11)	+	SI-4 (12)	+
207	SI-4 (13)	+	SI-4 (14)	+	SI-4 (15)	+
208	SI-4 (16)	+	SI-4 (17)	+	SI-4 (18)	+
209	SI-4 (19)	+	SI-4 (20)	+	SI-4 (21)	+
210	SI-4 (22)	+	SI-4 (23)	+	SI-4 (24)	+
211	SI-5	+	SI-5 (1)	+	SI-6	+
212	SI-6 (2)	+	SI-6 (3)	+	SI-7	+
213	SI-7 (1)	+	SI-7 (2)	+	SI-7 (3)	+
214	SI-7 (5)	+	SI-7 (6)	+	SI-7 (7)	+
215	SI-7 (8)	+	SI-7 (9)	+	SI-7 (10)	+
216	SI-7 (11)	+	SI-7 (12)	+	SI-7 (13)	+
217	SI-7 (14)	+	SI-7 (15)	+	SI-7 (16)	+
218	SI-8	+	SI-8 (1)	+	SI-8 (2)	+
219	SI-8 (3)	+	SI-10	+	SI-10 (1)	+
220	SI-10 (2)	+	SI-10 (3)	+	SI-10 (4)	+
221	SI-10 (5)	+	SI-11	+	SI-12	+
222	SI-13	+	SI-13 (1)	+	SI-13 (3)	+
223	SI-13 (4)	+	SI-13 (5)	+	SI-15	+
224	SI-17	+	PM-1	+	PM-2	+
225	PM-4	+	PM-5	+	PM-6	+
226	PM-8	+	PM-9	+	PM-10	+
227	PM-11	+	PM-14	+	PM-16	+

## **Detailed Guidance Control Specifications**

The following requirements for Control Documentation, Control Testing, and Evaluation of Test Results apply to all controls identified as required for financial statement audit readiness:

Control Documentation: See Appendix 1 (Section A.3) for documenting internal controls to comply with FIAR guidance requirements.

Control Testing: See Appendix 1 (Section A.5) for identifying test populations, testing techniques, appropriate sample sizes, and testing periods to comply with FIAR guidance requirements.

Evaluation of Test Results: See Appendix 1 (Section A.5) for acceptable number of test deviations and qualitative factors for consideration to comply with FIAR guidance requirements.

## **AC-1, ACCESS CONTROL POLICY AND PROCEDURES**

Justification to Select: System access control policies and procedures are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **AC-2.1.2**, **AS-1.1.1**, **AS-1.1.2**, **AS-1.3.1**, **AS-1.3.2**, **AS-1.4.1**, **AS-2.6.1**, and **AS-2.7.1**.

## **AC-2, ACCOUNT MANAGEMENT**

Justification to Select: Account management is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AS-3.1**, **AS-3.2.3**, **AC-3.1.1**, **AC-4.1.2**, **SD-1.1.7**, **SD-1.3.3**, **SD-2.2.1**, **SD-2.2.2**, **SD-2.2.3**, **SD-2.2.5**, **AS-1.1.2**, **AS-1.3.1**, **AS-2.4.1**, **AS-2.4.2**, **AS-2.4.3**, **AS-2.5.1**, **AS-2.6.2**, **AS-2.6.3**, **AS-2.6.4**, **AS-2.6.5**, **AS-3.8.1**, **AS-4.4.1**, **BP-3.5.1**, **BP-3.5.2**, **BP-4.7.1**, **DA-1.1.3**, and **DA-1.3.2**.

Parameter Values: e. Requires approvals by *resource owners* for requests to create information system accounts.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (7), (9), (10), (11), (12), and (13). Control enhancements (6) and (8) are not included as dynamic privilege management and dynamic account creation are operational requirements and not required controls for financial reporting.

## **AC-3, ACCESS ENFORCEMENT**

Justification to Select: Account enforcement is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.4**, **AC-2.1.16**, **AC-3.1.2**, **AC-4.1.3**, **AC-4.1.7**, **AC-4.2.1**, **AC-4.2.2**, **AC-4.2.3**, **AC-4.2.4**, **AC-4.2.5**, **AC-4.2.6**, **SD-1.1.7**, **SD-1.3.3**, **AS-1.1.2**, **AS-2.1.1**, **AS-2.4.2**, **AS-2.4.3**, **AS-2.7.1**, **AS-3.8.1**, **AS-4.2.1**, **AS-4.3.1**, and **IN-1.2.1**.

Applicable Control Enhancements: (2), (3), (4), (5), (7), (8), (9), and (10).

## **AC-4, INFORMATION FLOW ENFORCEMENT**

Justification to Select: Information flow enforcement is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.1**, **AC-1.1.2**, **AC-1.1.4**, **AC-5.3.9**, **SM-3.1.1**, **AS-2.1.1**, **AS-3.8.1**, **BP-1.5.1**, **BP-2.5.1**, **BP-2.6.1**, **BP-2.7.2**, **BP-2.8.1**, **BP-2.9.1**, **BP-3.3.1**, **BP-3.3.2**, **IN-1.2.1**, **IN-2.1.1**, **IN-2.2.1**, **IN-2.2.2**, **IN-2.3.1**.

Applicable Control Enhancements: (1), (2), (3), (7), (8), (9), (10), (11), (12), (17), (20), (21), and (22). Control enhancements (4), (5), (6), (13), (14), (15), (18), and (19) are not included as these enhancements are operational requirements and not required controls for financial reporting.

## **AC-5, SEPARATION OF DUTIES**

Justification to Select: The separation of duties is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-3.1.16**, **SD-1.1.1**, **SD-1.1.2**, **SD-1.1.3**, **SD-1.1.4**, **SD-1.1.5**, **SD-1.1.6**, **SD-1.3.3**, **SD-2.1.1**, **SD-2.1.2**, **SD-2.1.3**, **SD-2.2.1**, **SD-2.2.2**, **SD-2.2.3**, **SD-2.2.4**, **SD-2.2.5**, **AS-1.1.3**, **AS-1.3.2**, **AS-2.4.3**, **AS-2.6.1**, **AS-2.6.2**, **AS-2.6.3**, **AS-2.6.4**, **AS-2.6.6**, **AS-3.10.1**, **AS-3.11.1**, **AS-4.1.1**, **AS-4.1.2**, **AS-4.2.1**, **AS-4.3.1**, **AS-4.4.1**, **AS-4.4.2**, **AS-4.4.3**, **AS-4.5.1**, **AS-4.5.2**, **AS-4.5.3**, **BP-3.2.3**, **BP-3.5.2**, **BP-4.4.3**, and **DA-1.1.3**.



## **AC-6, LEAST PRIVILEGE**

Justification to Select: The enforcement of least privilege for access control is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-7.1.1, AC-3.1.1, AC-3.1.5, AC-3.1.6, AC-3.1.9, AC-3.2.1, AC-3.2.2, AC-3.2.3, AC-3.2.5, AC-4.1.1, AC-6.1.2, AS-1.1.2, AS-1.1.3, AS-1.3.2, AS-2.4.3, AS-2.6.1, AS-2.6.2, AS-2.6.3, AS-2.6.4, AS-2.6.6, AS-2.8.1, AS-3.10.1, AS-3.11.1, AS-4.1.1, AS-4.1.2, AS-4.2.1, AS-4.3.1, AS-4.4.1, AS-4.4.2, AS-4.4.3, AS-4.5.1, AS-4.5.2, AS-4.5.3, BP-1.3.1, BP-3.2.3, BP-3.5.1, BP-3.5.2, and DA-1.1.3.**

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), (9), and (10). Control enhancement (8) is not included as privilege levels for code execution is an operational requirement and not a required control for financial reporting.

## **AC-7, UNSUCCESSFUL LOGON ATTEMPTS**

Justification to Select: Enforcing limits on unsuccessful logon attempts is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.7** and **AS-2.3.2.**

Applicable Control Enhancements: None. Control enhancement (2) is not included as purging / wiping a mobile device is an operational requirement and not a required control for financial reporting.

## **AC-8, SYSTEM USE NOTIFICATION**

Justification to Select: Displaying a system use notification before granting access to an information system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-1.2.3.

## **AC-9, PREVIOUS LOGON (ACCESS) NOTIFICATION**

Justification to Select: Displaying a notification with the previous logon information is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-1.2.3, AC-2.1.2, **AC-2.1.3, AC-2.1.7, AC-3.1.3, and AC-3.1.4.**

Applicable Control Enhancements: (1). Control enhancements (2), (3), and (4) are not included as notification of account changes and additional logon information are operational requirements and not required controls for financial reporting.

## **AC-10, CONCURRENT SESSION CONTROL**

Justification to Select: Enforcing a concurrent session control for accounts or users is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-2.1.14 and AS-2.3.4.

## **AC-11, SESSION LOCKOUT**

Justification to Select: The enforcement of a session lock is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.2.1** and **AS-2.3.2.**

Guidance: OMB Memorandum M-06-16

Applicable Control Enhancements: (1).

## **AC-12, SESSION TERMINATION**

Justification to Select: The automatic termination of user sessions after conditions requiring a disconnect are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-1.2.2 and **AS-2.3.2**.

Applicable Control Enhancements: (1).

## **AC-14, PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**

Justification to Select: Restricting the actions permitted without identification or authentication is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-2.1.1**.

## **AC-16, SECURITY ATTRIBUTES**

Justification to Select: The enforcement of security attributes is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.15**, **AC-2.6.2**, **AC-3.1.1**, **AC-4.1.1** and AC-4.2.2.

Applicable Control Enhancements: (1), (2), (3), (4), and (10). Control enhancements (5), (6), (7), (8), and (9) are not included as these security attribute enhancements are operational requirements and not required controls for financial reporting.

## **AC-17, REMOTE ACCESS**

Justification to Select: The enforcement of usage restrictions on remote access is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.2**, AC-1.1.4, AC-1.1.5, AC-1.1.6, **AC-1.1.7**, **AC-2.1.3**, **AC-4.1.2**, **AC-4.1.3**, AC-4.3.1, and AC-4.3.2.

Applicable Control Enhancements: (1), (2), (3), (4), and (6). Control enhancement (9) is not included as disconnecting or disabling access and is an operational requirement and not a required control for financial reporting.

## **AC-18, WIRELESS ACCESS**

Justification to Select: Enforcement of usage restrictions on wireless access is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.1**, **AC-1.1.2**, AC-1.1.6, **AC-1.1.7**, and AC-4.3.2.

Applicable Control Enhancements: (1), (3), (4), and (5).

## **AC-19, ACCESS CONTROLS FOR MOBILE DEVICES**

Justification to Select: Usage restrictions on organization controlled mobile devices are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.7** and AC-4.3.2.

Applicable Control Enhancements: (5). Control enhancement (4) is not included as restrictions for classified information and is an operational requirement and not a required control for financial reporting.

## **AC-20, USE OF EXTERNAL INFORMATION SYSTEMS**

Justification to Select: Establishing terms and conditions to access the information system from external information systems is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-7.1.1**, **AC-1.1.7**, and **BP-1.2.1**.

Applicable Control Enhancements: (1), (2), (3), and (4).

## **AC-21, INFORMATION SHARING**

Justification to Select: The facilitation of information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organizational defined sharing circumstances is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **AC-3.1.1 - AC-3.1.10**, **AC-3.2.1 - AC-3.2.5**, and **AS-1.1.1**.

Applicable Control Enhancements: None. Control enhancements for information sharing are operational requirements and not required controls for financial reporting.

## **AC-22, PUBLICLY ACCESSIBLE CONTENT**

Justification to Select:

Prevention of nonpublic information on publicly available sites is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AS-2.5.1** and **AC-3.2.5**.

## **AC-23, DATA MINING PROTECTION**

Justification to Select:

Use of technique to adequately detect and protect against data mining is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **DA-1.2.1** and **DA-1.2.2**.

## **AC-24, ACCESS CONTROL DECISIONS**

Justification to Select:

The establishment of procedures for access control decisions prior to access enforcement is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.15**, **AC-2.1.18**, **AC-3.1.1 - AC-3.1.10**.

Applicable Control Enhancements: (1). Control enhancement (2) is not included since access control decisions based on no user or process identity is an operational requirement and not a required control for financial reporting.

## **AC-25 REFERENCE MONITOR**

Justification to Select:

Implementation of a reference monitor for defined access control activities is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-3.2.1 - AC-3.2.5**.

#### **AT-1, SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**

Justification to Select: A security awareness training policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **SM-4.1.1**, **SM-4.1.2**, **SM-7.1.1**, **AS-1.1.1**, **AS-1.4.1**, and **AS-1.4.2**.

#### **AT-2, SECURITY AWARENESS TRAINING**

Justification to Select: Providing security awareness training for information system users is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.1.1**, **SM-4.1.2**, **AC-1.1.2**, **AC-6.1.5**, **AC-6.1.7**, **SD-1.3.2**, and **AS-1.4.2**.  
Applicable Control Enhancements: (1) and (2).

#### **AT-3, ROLE BASED SECURITY TRAINING**

Justification to Select: Security training for personnel with assigned security roles and responsibilities is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.1.1**, **SM-4.1.2**, **AC-1.1.2**, **AC-6.1.1**, **AC-6.1.2**, **AC-6.4.3**, **SD-1.3.2**, **CM-1.1.1**, **CP-2.2.9**, **CP-2.3.1**, **CP-2.3.2**, and **AS-1.4.2**.  
Applicable Control Enhancements: (1), (2), (3), and (4).

#### **AT-4, SECURITY TRAINING RECORDS**

Justification to Select: Documentation and monitoring of individual security training activities security training records is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.1.1**, **SM-4.3.2**, and **AC-6.1.5**.

#### **AU-1, AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**

Justification to Select: Documentation and implementation of audit and accountability policies and procedures is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **AS-1.1.1**, **AS-1.4.1**, **AS-2.8.1**, and **BP-2.9.2**.

#### **AU-2, AUDIT EVENTS**

Justification to Select: Identification of auditable events is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.2.2**, **AC-5.2.3**, **AS-2.8.1**, **BP-2.2.1**, **BP-2.2.2**, and **BP-2.2.3**.  
Applicable Control Enhancements: (3).

#### **AU-3, CONTENT OF AUDIT RECORDS**

Justification to Select: The content of the audit records identifying what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.2.4**, **AS-2.9.1**, **BP-2.2.1**, **BP-2.2.2**, **BP-2.2.3**, and **BP-2.9.2**.  
Applicable Control Enhancements: None. Control enhancements for content of audit records are operational requirements and not required controls for financial reporting.

#### **AU-4, AUDIT STORAGE CAPACITY**

Justification to Select: The allocation of sufficient audit record storage capacity to prevent capacity from being exceeded is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.2.5**.

Applicable Control Enhancements: (1).

#### **AU-5, RESPONSE TO AUDIT PROCESSING FAILURES**

Justification to Select: Response to audit processing failures is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.2.5** and **DA-1.2.2**.

Applicable Control Enhancements: (1) and (2). Control enhancements (3) and (4) are not included as these configurable traffic volume thresholds and shutdown on failure enhancements are operational requirements and not required controls for financial reporting.

#### **AU-6, AUDIT REVIEW, ANALYSIS, AND REPORTING**

Justification to Select: Review and analysis of information system audit records, with reporting on findings, is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-3.1.1**, **AC-3.1.6**, **AC-5.2.6**, **SD-2.2.1**, **SD-2.2.3**, **SD-2.2.5**, **AS-2.9.1**, **AS-2.10.1**, **BP-2.9.2**, **BP-2.9.3**, **BP-2.9.4**, **IN-2.4.1**, **IN-2.5.3**, and **DA-1.2.1**.

Applicable Control Enhancements: (1), (7) and (10). Control enhancements (3), (4), (5), (6), (8), and (9) are not included as these audit review, analysis and reporting enhancements are operational requirements and not required controls for financial reporting.

#### **AU-7, AUDIT REDUCTION AND REPORT GENERATION**

Justification to Select: Audit reduction and report generation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.2.4**, **AC-5.2.6**, and **AS-2.10.1**.

Applicable Control Enhancements: (1). Control enhancement (2) is not included as automatic sort and search is an operational requirement and not a required control for financial reporting.

#### **AU-8, TIME STAMPS**

Justification to Select: Time stamps for audit records are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.2.4**.

Applicable Control Enhancements: (1). Control enhancement (2) is not included as a secondary authoritative time source is an operational requirement and not a required control for financial reporting.

## **AU-9, PROTECTION OF AUDIT INFORMATION**

Justification to Select: Protection of audit information and audit tools from unauthorized access, modification, or deletion is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-4.3.1, **AC-5.2.6**, **AC-5.2.7**, **CP-2.1.1**, and CP-2.1.3.

Applicable Control Enhancements: (2), (4), and (6). Control enhancements (1), (3), and (5) are not included as protection of audit information enhancements are operational requirements and not required controls for financial reporting.

## **AU-10, NON-REPUDIATION**

Justification to Select: Non-repudiation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.1**, **AC-5.2.4**, **AC-2.1.15**, and **DA-2.1.1**.

Applicable Control Enhancements: (1), (2), (3), and (4).

## **AU-11, AUDIT RECORD RETENTION**

Justification to Select: Audit record retention is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.2.7**.

Applicable Control Enhancements: None. Control enhancement (1) is not included long-term retrieval capability is an operational requirement and not a required control for financial reporting.

## **AU-12, AUDIT GENERATION**

Justification to Select: Audit record generation for defined security events is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.2.3** and **AC-5.2.6**.

Applicable Control Enhancements: (3). Control enhancements (1) and (2) are not included as these audit generation enhancements are operational requirements and not required controls for financial reporting.

## **CA-1, SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES**

Justification to Select: Security assessment and authorization policy and procedures are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-1.4.1**, **SM-1.4.2**, **SM-2.1.1**, **SM-3.1.1**, **SM-5.1.1**, **AS-1.1.1**, AS-1.4.1, AS-1.5.1, **AS-1.5.2**, and AS-1.5.3.

## **CA-2, SECURITY ASSESSMENTS**

Justification to Select: Security assessment and authorization policy and procedures are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.3**, **SM-2.1.4**, SM-2.1.6, **SM-5.1.1**, SM-5.1.4, SM-5.1.5, SM-5.1.6, SM-5.1.7, **AC-1.1.2**, AC-6.1.7, AC-6.5.4, CP-2.2.9, AS-1.5.1, **AS-1.5.2**, and AS-1.5.3.

Applicable Control Enhancements: (1), (2), and (3).

### **CA-3, SYSTEM INTERCONNECTIONS**

Justification to Select: Use of Interconnection Security Agreements to authorize connections to other information systems is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.1**, **AC-1.1.2**, **AC-1.1.4**, **AC-3.2.5**, **IN-1.1.1**, **IN-1.2.1**, **IN-2.1.1**, **IN-2.2.1**, **DA-1.1.1**, and **DA-1.3.2**.

Applicable Control Enhancements: (1), (3), (4), and (5). Control enhancement (2) is not included as having classified national security system connections is an operational requirement and not a required control for financial reporting.

### **CA-5, PLAN OF ACTIONS AND MILESTONES**

Justification to Select: Development and updating of plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-6.1.1**, **SM-6.1.2**, **SM-6.1.3**, **AS-1.6.1**, **AS-1.6.2**, **AS-1.6.3**, and **AS-1.6.4**.

Applicable Control Enhancements: None.

### **CA-6, SECURITY AUTHORIZATION**

Justification to Select: The authorization of an information system processing before being placed into operation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.4** and **SM-2.1.6**.

### **CA-7, CONTINUOUS MONITORING**

Justification to Select: The authorization of an information system processing before being placed into operation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.6**, **SM-5.1.1**, **SM-5.1.6**, **AS-1.6.4**, **AS-2.8.1**, **IN-2.2.3**, **DA-1.2.1**, and **DA-1.2.2**.

Applicable Control Enhancements: (1). Control enhancement (3) is not included as trend analysis is an operational requirement and not a required control for financial reporting.

### **CA-8, PENETRATION TESTING**

Justification to Select: Use of penetration testing to support risk assessment activities is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.3**, **AS-1.1.1**, and **AS-1.5.2**.

Applicable Control Enhancements: (1). Control enhancement (2) is not included as the use of red team exercises is an operational requirement and not a required control for financial reporting.

### **CA-9 INTERNAL SYSTEM CONNECTIONS**

Justification to Select: Authorization and documentation of internal system connections is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.1**, **IN-1.1.1**, and **IN-2.1.1**.

Applicable Control Enhancements: (1).

## **CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**

Justification to Select: The organization development and documentation of policies, policies, plans and procedures is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1, SM-1.1.2, SM-1.2.1, SM-3.1.1, CM-1.1.1, CM-2.1.1, CM-3.1.1, CM-4.1.3, CM-6.1.1, CM-6.2.1, AS-1.1.1, AS-1.4.1, AS-3.1.1, AS-3.3.1, and BP-4.2.1.**

## **CM-2 BASELINE CONFIGURATION**

Justification to Select: The organization development, documentation and maintenance under configuration control, of a current baseline configuration for the information system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-2.1.1, CM-2.1.3, CM-4.1.1, CM-4.1.2, AS-3.2.1, and AS-3.12.1.**  
Applicable Control Enhancements: (1). Control enhancements (2), (3), (6), and (7) are not included as these baseline configuration enhancements are operational requirements and not required controls for financial reporting.

## **CM-3 CONFIGURATION CHANGE CONTROL**

Justification to Select: The organizations configuration control of information systems involving the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications, is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.3.1, AC-2.1.13, AC-2.1.16, CM-1.1.1, CM-3.1.2, CM-3.1.3, CM-3.1.4, CM-3.1.7, CM-3.1.8, CM-3.1.13, CM-3.1.14, CM-3.1.15, CM-3.1.18, CM-6.1.1, CM-6.2.1, AS-3.4.1, AS-3.4.2, AS-3.5.1, AS-3.5.2, AS-3.5.3, AS-3.5.4, AS-3.5.5, AS-3.5.6, AS-3.5.7, AS-3.5.8, AS-3.5.9, AS-3.6.1, AS-3.7.1, AS-3.9.1, AS-3.12.1, AS-3.14.1, BP-4.2.2, BP-4.2.3, BP-4.4.1, BP-4.4.2, BP-4.4.4, BP-4.5.1, BP-4.6.1, BP-4.6.2, IN-1.2.2, and IN-2.2.2.**

Applicable Control Enhancements: (2), (4), and (6). Control enhancements (1), (3), and (5) are not included as automated configuration change control enhancements are operational requirements and not required controls for financial reporting.

## **CM-4 SECURITY IMPACT ANALYSIS**

Justification to Select: Analyzing changes to the information system to determine potential security impacts prior to change implementation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-3.1.5, CM-3.1.6, CM-3.1.7, CM-3.1.8, CM-3.1.9, CM-3.1.10, CM-3.1.11, CM-3.1.12, CM-3.1.16, CM-4.1.4, AS-3.5.1, AS-3.5.2, AS-3.5.3, AS-3.5.4, AS-3.5.5, AS-3.5.6, AS-3.5.7, AS-3.5.8, AS-3.5.9, AS-3.6.1, AS-3.6.2, AS-3.7.1, AS-3.10.1, BP-4.4.4, BP-4.6.1, BP-4.6.2, IN-1.2.2, and IN-2.2.2.**

Applicable Control Enhancements: (1) and (2).



## **CM-5 ACCESS RESTRICTIONS FOR CHANGE**

Justification to Select: Defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the information system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-3.1.2**, **CM-3.1.12**, **CM-3.1.16**, **CM-3.1.17**, **AS-3.4.2**, **AS-3.5.3**, **AS-3.6.2**, **AS-3.6.3**, **AS-3.7.1**, **AS-3.8.1**, **AS-3.9.1**, **AS-3.12.1**, and **BP-1.5.3**.

Applicable Control Enhancements: (1), (2), (4), (5), and (6). Control enhancement (3) is not included as signed components are an operational requirement and not a required control for financial reporting.

## **CM-6 CONFIGURATION SETTINGS**

Justification to Select: Establishment and documentation of configuration settings is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-2.1.3**, **CM-4.1.4**, **AS-3.2.1**, **AS-3.11.1**, and **AS-3.12.1**.

Applicable Control Enhancements: (1) and (2).

## **CM-7 LEAST FUNCTIONALITY**

Justification to Select: The configuration of systems to only provide essential capabilities is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.5.1**, **AC-3.1.7**, **AC-3.1.9**, **AC-3.2.1**, **AC-3.2.2**, **AC-3.2.3**, **CM-2.1.3**, **CM-4.1.1** and **AS-4.2.1**.

Applicable Control Enhancements: (1), (2), and (3). Control enhancements (4) and (5) are not included as blacklisting and whitelisting are operational requirements and not required controls for financial reporting.

## **CM-8 INFORMATION SYSTEM COMPONENT INVENTORY**

Justification to Select: Developing and documenting an information system component inventory is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.3.1**, **SM-1.5.1**, **CM-2.1.1**, and **CM-2.1.2**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), and (9). Control enhancement (8) is not included as signed components are an operational requirement and not a required control for financial reporting.

## **CM-9 CONFIGURATION MANAGEMENT PLAN**

Justification to Select: Developing, documenting and implementing configuration management plans is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-1.1.1**, **CM-3.1.1**, **CM-4.1.3**, **SD-1.1.2**, **AS-3.1.1**, and **AS-3.3.1**.

Applicable Control Enhancements: (1).

## **CM-10 SOFTWARE USAGE RESTRICTIONS**

Justification to Select: Software usage restrictions are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CM-3.1.19, CM-5.1.7, and CM-5.1.8.

Applicable Control Enhancements: None. Control enhancement (1) is not included as open source software restrictions are an operational requirement and not a required control for financial reporting.

## **CM-11 USER-INSTALLED SOFTWARE**

Justification to Select: Establishing policies for monitoring and enforcing restrictions on user-installed software is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CM-3.1.19 and CM-5.1.8.

Applicable Control Enhancements: (1) and (2).

## **CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES**

Justification to Select: Contingency planning policies and procedures are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **AS-1.1.1**, **AS-1.4.1**, **AS-5.3.2**, and **CP-3.1.1**.

## **CP-2 CONTINGENCY PLAN**

Justification to Select: Developing contingency plans that identify essential missions and business functions and associated contingency requirements is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.5.1, **CP-1.1.2**, **CP-1.2.1**, **CP-1.2.2**, **CP-1.3.1**, **CP-2.1.3**, **CP-2.1.4**, CP-2.3.3, CP-3.1.1, CP-3.1.2, CP-3.1.3, CP-3.1.4, CP-3.1.5, CP-3.1.6, CP-3.1.7, CP-3.2.1, CP-3.2.3, **AS-5.1.1**, **AS-5.1.2**, **AS-5.1.3**, **AS-5.3.1**, **AS-5.3.2**, and **AS-5.3.3**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), and (8).

## **CP-3 CONTINGENCY TRAINING**

Justification to Select: Providing contingency training for information system users, commensurate with their responsibility, is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.3.1, CP-2.3.2, CP-4.1.1, and **AS-5.4.1**.

Applicable Control Enhancements: (1) and (2).

## **CP-4 CONTINGENCY PLAN TESTING**

Justification to Select: Testing contingency plans to determine the effectiveness of the plan and organizational readiness to execute the plan is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.5.1, CP-2.2.9, CP-2.1.3, **CP-2.1.4**, CP-2.3.4, CP-3.1.7, CP-4.1.1, CP-4.2.1, CP-4.2.2, **AS-5.4.1**, **AS-5.4.2**, **AS-5.4.3**, and **AS-5.4.4**.

Applicable Control Enhancements: (1), (2), (3), and (4).

## **CP-6 ALTERNATE STORAGE SITE**

Justification to Select: Establishing an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information and ensuring the alternate storage site provides information security safeguards equivalent to the primary site is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-2.1.1**, CP-2.1.2, CP-2.1.3, CP-3.2.1, CP-3.2.2, AS-5.1.2, **AS-5.2.3**.

Applicable Control Enhancements: (1), (2), and (3).

## **CP-7 ALTERNATE PROCESSING SITE**

Justification to Select: Establishing an alternative processing site to permit the transfer and resumption of critical business functions while the primary processing capabilities are unavailable is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-3.2.1, CP-3.2.2, CP-2.1.3, CP-3.2.2, **AS-5.2.3**, and **AS-5.4.2**.

Applicable Control Enhancements: (1), (2), (3), (4), and (6).

## **CP-8 TELECOMMUNICATIONS SERVICES**

Justification to Select: Establishing alternate telecommunications services, including necessary agreements to permit the resumption of information systems operations for essential missions and business functions when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites, is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-3.2.1 and CP-3.2.2.

Applicable Control Enhancements: (1), (2), (3), (4), and (5).

## **CP-9 INFORMATION SYSTEM BACKUP**

Justification to Select: Backups of user-level information, system-level information and information system documentation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-2.1.1**, CP-2.1.2, **CP-2.1.4**, CP-2.4.5, CP-3.2.1, CP-3.2.2, **AS-5.2.1**, **AS-5.2.2**, and **AS-5.2.3**.

Applicable Control Enhancements: (1), (2), (3), (5), and (6). Control enhancement (7) is not included as dual authorization is an operational requirement and not a required control for financial reporting.

## **CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**

Justification to Select: Information system recovery and reconstitution to a known state after information system disruption, compromise or failure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-2.1.1**, CP-2.1.3, **CP-2.1.4**, AS-5.1.2, **AS-5.2.3**, and **AS-5.3.3**.

Applicable Control Enhancements: (2), (4), and (6).

## **IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**

Justification to Select: The organization must develop, document, disseminate, review, and update the identification and authentication policies and procedures that address the following:

- Purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls for the information system

This is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **AC-2.1.2**, **AC-2.1.3**, **AS-1.1.1**, **AS-1.4.1**, **AS-2.2**, and **AS-2.3.1**.

## **IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**

Justification to Select: Systems(s) must uniquely identify and authenticate users and processes to the system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.1**, **AC-2.1.4**, **AC-2.1.9**, **AC-2.1.18**, **AC-4.1.1**, **AS-2.2**, and **AS-2.3.2**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), (8), (9), (10), (11), (12), and (13).

## **IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION**

Justification to Select: Device identification and authentication is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.3** and **AC-1.1.5**.

Applicable Control Enhancements: (1), (3), and (4).

## **IA-4 IDENTIFIER MANAGEMENT**

Justification to Select: Identifier management is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques, **AC-2.1.1**, **AC-2.1.2**, and **AC-2.1.3** and **AS-2.3.3**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), and (7).

## **IA-5 AUTHENTICATOR MANAGEMENT**

Justification to Select: Authenticator management is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.4**, **AC-2.1.5**, **AC-2.1.6**, **AC-2.1.7**, **AC-2.1.8**, **AC-2.1.9**, **AC-2.1.10**, **AC-2.1.11**, **AC-2.1.12**, **AC-2.1.13**, **AC-2.1.15**, **AC-2.1.16**, **AC-2.1.17**, **AC-3.1.7**, **AC-3.2.3**, **AC-4.1.3**, **AC-4.1.5**, and **AS-2.3.1**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), (8), (9), (10), (11), (12), (13), (14), and (15).

## **IA-6 AUTHENTICATOR FEEDBACK**

Justification to Select: Authenticator feedback is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-2.1.17**.

## **IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION**

Justification to Select: Cryptographic module is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-4.3.3 and **AC-2.1.16**.

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

Justification to Select: Systems(s) must uniquely identify and authenticate users and a process to the system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-2.1.1** and AC-2.1.2.

Applicable Control Enhancements: (1), (2), (3), (4), and (5).

## **IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION**

Justification to Select: System(s) must uniquely identify and authenticate services to the system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-7.1.1**, **AC-1.1.3**, and AC-2.1.1.

Applicable Control Enhancements: (1) and (2).

## **IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION**

Justification to Select: Adaptive identification and authentication is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-2.1.4.

## **IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES**

Justification to Select: Incident response policy and procedures are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-3.1.1**, **AC-5.1.1**, AC-5.3.7, **AS-1.1.1**, and AS-1.4.1.

## **IR-2 INCIDENT RESPONSE TRAINING**

Justification to Select: Incident response training is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.1.1**, CP4.1.1 and **AS-5.4.1**.

Applicable Control Enhancements: (1). Control enhancement (2) is not included as automated training environments is an operational requirement and not a required control for financial reporting.

## **IR-3 INCIDENT RESPONSE TESTING**

Justification to Select: Incident response testing is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.1.1** and CP-3.1.1.

Applicable Control Enhancements: (2). Control enhancement (1) is not included as automated testing is an operational requirement and not a required control for financial reporting.

## **IR-4 INCIDENT HANDLING**

Justification to Select: Incident response handling is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.1.1**, **AC-5.3.1**, **AC-5.3.2**, AC-5.3.6, and AC-5.3.7.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), (8), (9), and (10).

## **IR-5 INCIDENT MONITORING**

Justification to Select: Incident monitoring is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-5.2.2, **AC-5.2.3**, **AC-5.2.7** and **AC-5.3.4**.

Applicable Control Enhancements: (1).

## **IR-6 INCIDENT REPORTING**

Justification to Select: Incident reporting is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.3.1**, **AC-5.3.2**, **AC-5.3.4**, and AC-5.3.6.

Applicable Control Enhancements: (1), (2), and (3).

## **IR-7 INCIDENT RESPONSE ASSISTANCE**

Justification to Select: Incident response assistance is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.1.1**.

Applicable Control Enhancements: (2). Control enhancement (1) is not included as automation support for availability of information is an operational requirement and not a required control for financial reporting.

## **IR-8 INCIDENT RESPONSE PLAN**

Justification to Select: Incident response plan is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.1.1**.

## **IR-9 INFORMATION SPILLAGE RESPONSE**

Justification to Select: Information spillage response plan is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.3.1** - AC-5.3.9, **SM-1.1.1** and **SM-4.1.1**.

Applicable Control Enhancements: (1), (2), (3), and (4).

## **IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM**

Justification to Select: Integrated information security analysis is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-5.3.9.

## **MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES**

Justification to Select: System maintenance policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-3.1.1**, CP-2.4.1, CP-2.4.6, **AS-1.1.1**, and AS-1.4.1.

## **MA-2 CONTROLLED MAINTENANCE**

Justification to Select: Controlled maintenance is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.4.9, CP-2.4.2, CP-2.4.3, CP-2.4.4, CP-2.4.7, CP-2.4.8, CP-2.4.10, and CP-2.4.11.

Applicable Control Enhancements: (2).

#### **MA-4 NONLOCAL MAINTENANCE**

Justification to Select: Nonlocal maintenance is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.1.3**, **SM-7.1.1**, **SM-7.1.2** and **SD-1.1.2**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), and (7).

#### **MA-6 TIMELY MAINTENANCE**

Justification to Select: Timely maintenance is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-2.4.2**, **CP-2.4.5**, **CP-2.4.10** and **CP-2.4.11**.

Applicable Control Enhancements: (1), (2), and (3).

#### **MP-1 MEDIA PROTECTION POLICY AND PROCEDURES**

Justification to Select: Media protection policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **AS-1.1.1**, and **AS-1.4.1**.

#### **MP-2 MEDIA ACCESS**

Justification to Select: Media access is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-4.2.1**.

#### **MP-3 MEDIA MARKETING**

Justification to Select: Media marketing is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-4.2.2**.

#### **MP-4 MEDIA STORAGE**

Justification to Select: Media storage is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.2.4**, **AC-6.4.8**, and **AC-6.4.9**.

Applicable Control Enhancements: (2).

#### **MP-5 MEDIA TRANSPORT**

Justification to Select: Media transport is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.2.3**, **AC-4.2.4**, **AC-4.3.1**, and **AC-6.3.7**.

Applicable Control Enhancements: (3) and (4).

#### **MP-6 MEDIA SANITIZATION**

Justification to Select: Media sanitization is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-4.2.6**.

Applicable Control Enhancements: (1), (2), (3), (7), and (8).

#### **MP-7 MEDIA USE**

Justification to Select: Media sanitization is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.7** and **SM-4.1.2**.

Applicable Control Enhancements: (1) and (2).

#### **MP-8 MEDIA DOWNGRADING**

Justification to Select: Downgrading of classified information removed from media intended for wider release and distribution outside the organization is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-4.2.1, AC-4.2.2, AC-4.2.3, AC-4.2.4, **AC-4.2.5**, and AC-4.2.6.  
Applicable Control Enhancements: (1), (2), (3) and (4).

## **PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**

Justification to Select: Physical and environmental protection policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-3.1.1**, AC-6.1.1, **AC-6.1.2**, **AS-1.1.1**, AS-1.4.1, AS-2.11.1, and **DA-1.1.2**.

## **PE-2 PHYSICAL ACCESS AUTHORIZATIONS**

Justification to Select: Physical access authorization is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.1.9, **AC-6.3.1**, **AC-6.3.2**, **AC-6.3.3**, AC-6.4.2, **AC-6.4.4**, AS-2.11.1, and **DA-1.1.2**.  
Applicable Control Enhancements: (1), (2), and (3).

## **PE-3 PHYSICAL ACCESS CONTROL**

Justification to Select: Physical access control is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-6.1.2**, AC-6.1.8, AC-6.1.9, AC-6.2.1, AC-6.2.2, AC-6.2.3, AC-6.2.5, **AC-6.3.2**, AC-6.3.4, AC-6.3.7, AC-6.3.8, AC-6.4.2, **AC-6.4.3**, **AC-6.4.4**, AC-6.4.6, AC-6.4.7, AC-6.5.2, AS-2.11.1, **DA-1.1.1**, and **DA-1.1.2**.  
Applicable Control Enhancements: (1), (2), (3), (4), (5), and (6).

## **PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM**

Justification to Select: Access control for transmission medium is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.4.8 and AC-4.2.3.

## **PE-5 ACCESS CONTROL FOR OUTPUT DEVICES**

Justification to Select: Access control for output devices is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-4.2.1, AC-4.2.3, **AC-6.3.2** and **AC-6.4.3**.  
Applicable Control Enhancements: (1), (2), and (3).

## **PE-6 MONITORING PHYSICAL ACCESS**

Justification to Select: Access control for output devices is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.1.7, AC-6.2.3, AC-6.3.4, AC-6.3.5, AC-6.3.8, **AC-6.3.3**, **AC-6.4.3**, **AC-6.4.4**, AC-6.4.5, AC-6.5.3, AS-2.11.1, and **DA-1.1.2**.  
Applicable Control Enhancements: (1), (2), (3), and (4).

## **PE-8 VISITOR ACCESS RECORDS**



Justification to Select: Access control for output devices is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.1.9, AC-6.3.5, and AC-6.4.2.

Applicable Control Enhancements: (1).

## **PE-9 POWER EQUIPMENT AND CABLING**

Justification to Select: Power equipment and cabling is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.2, CP-2.2.3, CP-2.2.6, **AC-6.4.3**, and AC-6.4.10.

Applicable Control Enhancements: (1) and (2).

## **PE-10 EMERGENCY SHUTOFF**

Justification to Select: Emergency shutoff is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.2 and CP-2.2.8.

## **PE-11 EMERGENCY POWER**

Justification to Select: Emergency power is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.4.10, CP-2.2.2, CP-2.2.3, and CP-2.2.5.

Applicable Control Enhancements: (1) and (2).

## **PE-12 EMERGENCY LIGHTING**

Justification to Select: Emergency lighting is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-6.2.4, CP-2.2.2, and CP-2.2.7.

Applicable Control Enhancements: (1).

## **PE-13 FIRE PROTECTION**

Justification to Select: Fire protection is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.1, CP-2.2.2, and CP-2.2.9.

Applicable Control Enhancements: (1), (2), (3), and (4).

## **PE-14 TEMPERATURE AND HUMIDITY CONTROLS**

Justification to Select: Temperature and humidity control is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.3 and CP-2.2.6.

Applicable Control Enhancements: (1) and (2).

## **PE-15 WATER DAMAGE PROTECTION**

Justification to Select: Water damage protection is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.1, CP-2.2.2, and CP-2.2.4.

Applicable Control Enhancements: (1).

## **PE-16 DELIVERY AND REMOVAL**

Justification to Select: Delivery and removal is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-6.3.7.

## **PE-17 ALTERNATE WORK SITE**

Justification to Select: Alternate work site is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.2, CP-2.2.3, CP-3.2.2, and CP-3.2.3.

#### **PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS**

Justification to Select: Location of information system components is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques CP-2.2.2 and CP-2.2.4.

Applicable Control Enhancements: (1).

#### **PL-1 SECURITY PLANNING POLICY AND PROCEDURES**

Justification to Select: Security planning policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **AS-1.1.1**, **AS-1.4.1**, and **AS-1.5.4**.

#### **PL-2 SYSTEM SECURITY PLAN**

Justification to Select: System security plan is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-1.2.2**, **SM-1.3.1**, **SM-1.4.1**, **SM-1.4.2**, **SM-3.1.1**, **CM-5.1.2**, **CM-5.1.4**, **AS-1.1.1**, and **AS-2.1.1**.

Applicable Control Enhancements: (3).

#### **PL-4 RULES OF BEHAVIOR**

Justification to Select: Rules of behavior is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.1.1**, **SM-4.1.2**, and **CP-2.2.10**.

Applicable Control Enhancements: (1).

#### **PL-7 SECURITY CONCEPT OF OPERATIONS**

Justification to Select: Security concept of operations is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-3.1.1**.

#### **PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES**

Justification to Select: Personnel security policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **SM-4.1.1**, and **AS-1.1.1**.

#### **PS-2 POSITION RISK DESIGNATION**

Justification to Select: Position risk designation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.2.1** and **SM-4.2.2**.

### **PS-3 PERSONNEL SCREENING**

Justification to Select: Personnel screening is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques SM-4.2.1 and SM-4.2.2.

Applicable Control Enhancements: (1), (2), and (3).

### **PS-4 PERSONNEL TERMINATION**

Justification to Select: Personnel termination is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-4.2.6**.

Applicable Control Enhancements: (1) and (2).

### **PS-5 PERSONNEL TRANSFER**

Justification to Select: Personnel transfer is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-4.2.6**.

### **PS-6 ACCESS AGREEMENT**

Justification to Select: Access Agreement is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques SM-4.1.2, SM-4.2.3, and **SM-4.2.6**.

Applicable Control Enhancements: (2) and (3).

### **PS-7 THIRD-PARTY PERSONNEL SECURITY**

Justification to Select: Third-party personnel security is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-7.1.1**, SM-7.1.2, AC-6.1.6, **AS-1.7.1**, and AS-1.7.2.

### **PS-8 PERSONNEL SANCTIONS**

Justification to Select: Personnel sanctions are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.2.5** and **AC-5.3.3**.

### **RA-1 RISK ASSESSMENT POLICY AND PROCEDURES**

Justification to Select: Risk assessment policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-2.1.1**, **SM-3.1.1**, **AS-1.1.1**, **AS-1.2.1**, and AS-1.4.1.

### **RA-2 SECURITY CATEGORIZATION**

Justification to Select: Security categorization is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.2**, **CP-1.1.1**, and **CP-1.1.2**.

### **RA-3 RISK ASSESSMENT**

Justification to Select: Risk assessment is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.3**, **SM-2.1.4**, **SM-2.1.5**, AC-6.1.1, AC-6.1.3, AC-6.5.4, and **AS-1.2.1**.

## **RA-5 VULNERABILITY SCANNING**

Justification to Select: Vulnerability scanning is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-5.1.2**, **CM-5.1.1**, and **AS-3.13.1**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (8), and (10).

## **RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY**

Justification to Select: Technical surveillance countermeasures survey is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-2.1.1** and **AS-1.2.1**.

## **SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**

Justification to Select: System and services acquisition policy and procedure is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **SM-7.1.1**, **AS-1.1.1**, and **AS-1.4.1**.

## **SA-2 ALLOCATION OF RESOURCES**

Justification to Select: Allocation of resources is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-1.2.1**.

## **SA-3 SYSTEM DEVELOPMENT LIFE CYCLE**

Justification to Select: System development life cycle is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AS-3.3.1**.

## **SA-4 ACQUISITION PROCESS**

Justification to Select: Acquisition Process is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-7.1.2**.

Applicable Control Enhancements: (1), (2), (3), (5), (6), (7), (8), (9), and (10).

## **SA-5 INFORMATION SYSTEM DOCUMENTATION**

Justification to Select: Information system documentation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **CM-2.1.1**, and **AS-1.1.1**.

## **SA-8 SECURITY ENGINEERING PRINCIPLES**

Justification to Select: Security engineering principles is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **CM-1.1.1**.

## **SA-9 EXTERNAL INFORMATION SYSTEM**

Justification to Select: External information system is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-7.1.1**, **SM-7.1.2**.

Applicable Control Enhancements: (1), (2), (3), (4), and (5).

## **SA-10 DEVELOPER CONFIGURATION MANAGEMENT**

Justification to Select: Developer configuration management is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-1.1.1**, **CM-3.1.14**, **CM-3.1.15**, **CM-3.1.17**, and **CM-3.1.18**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), and (6).

## **SA-11 DEVELOPER SECURITY TESTING AND EVALUATION**

Justification to Select: Developer security testing and evaluation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-1.1.1**, **CM-3.1.5**, **CM-3.1.6**, **CM-3.1.7**, **CM-3.1.8**, **CM-3.1.9**, **CM-3.1.10**, **CM-3.1.11**, and **CM-3.1.12**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), and (8).

## **SA-12 SUPPLY CHAIN PROTECTION**

Justification to Select: Supply chain protection is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-6.1.1**, **SM-7.1.1**, **SM-7.1.2**, **CM-1.1.1**, and **AS-1.1.1**.

Applicable Control Enhancements: (1), (2), (5), (7), (8), (9), (10), (11), (12), (13), (14), and (15).

## **SA-13 TRUSTWORTHINESS**

Justification to Select: Trustworthiness is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-1.1.1** and **AS-1.1.1**.

## **SA-14 CRITICALITY ANALYSIS**

Justification to Select: Criticality analysis is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AS-1.1.1**.

## **SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS**

Justification to Select: Development process, standards, and tools are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-7.1.1**, **SM-7.1.2**, **CM-1.1.1**, and **CM-3.1.16**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), (7), (8), (9), (10), and (11).

## **SA-16 DEVELOPER-PROVIDED TRAINING**

Justification to Select: Developer provided training is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-4.3.2**.

## **SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN**

Justification to Select: Developer security architecture and design is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-1.1.1**, **SM-7.1.1**, and **SM-7.1.2**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (6), and (7).

## **SA-18 TAMPER RESISTANCE AND DETECTION**

Justification to Select: Tamper resistance and detection is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.3.8**.

Applicable Control Enhancements: (1) and (2).

## **SA-21 DEVELOPER SCREENING**

Justification to Select: Developer screening is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques SM-4.2.1, SM-4.2.2, and **AC-3.1.1**.

Applicable Control Enhancements: (1).

## **SC-1 SYSTEMS AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**

Justification to Select: The development, communication, and maintenance of policy and procedures for effective implementation of selected security controls and control enhancements are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-3.1.1**, **AS-1.1.1**, and AS-1.4.1.

## **SC-2 APPLICATION PARTITIONING**

Justification to Select: Separation of user functionality (including user interface services) from information system management functionality is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-4.1.8**.

Applicable Control Enhancements: (1).

## **SC-3 SECURITY FUNCTION ISOLATION**

Justification to Select: Separation of security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-4.1.9**.

Applicable Control Enhancements: (1), (2), (3), (4), and (5).

## **SC-5 DENIAL OF SERVICE PROTECTION**

Justification to Select: Protecting systems against or limiting the effects of denial of service attacks by using organization-defined security safeguards is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-5.1.1**.

Applicable Control Enhancements: (1), (2), and (3).

## **SC-6 RESOURCE AVAILABILITY**

Justification to Select: Protecting the availability of resources by priority, quota or other means is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques SM-1.2.1 and **CP-1.2.2**.

## **SC-7 BOUNDARY PROTECTION**

Justification to Select: Monitoring and controlling communication at the external boundary of the system and at key internal boundaries within the system, implementing subnetworks for publically accessible system components that are separated from the internal organizational networks, and connecting to external networks or information systems only through managed interfaces in accordance with the organization's security architecture are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.1**, **AC-1.1.2**, **AC-3.2.1**, **AC-4.1.9**, **AC-6.1.2**, **AC-6.1.8**, **CP-2.4.5**, **CP-2.4.6**, **AS-2.1.1**, and **AS-2.5.1**.

Applicable Control Enhancements: (3), (4), (5), (7), (8), (9), (10), (11), (12), (13), (14), (15), (16), (17), (18), (19), (20), (21), (22), and (23).

## **SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY**

Justification to Select: Safeguards to protect transmitted information are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.3.1** and **AC-4.3.2**.

Applicable Control Enhancements: (1), (2), (3), and (4).

## **SC-10 NETWORK DISCONNECT**

Justification to Select: Terminating the network connection associated with a communications session at the end of the session or after a specified period of inactivity is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-1.2.2**.

## **SC-11 TRUSTED PATH**

Justification to Select: Establishing trusted communications paths between the user and the system security functions such as authentication and re-authentication is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-4.1.10**.

Applicable Control Enhancements: (1).

## **SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**

Justification to Select: Establishing and managing cryptographic keys for required cryptography employed within the information system in accordance with DoD requirements for key generation, distribution, storage, access, and destruction is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.3.1** and **AC-4.3.4**.

Applicable Control Enhancements: (1), (2), and (3).

## **SC-13 CRYPTOGRAPHIC PROTECTION**

Justification to Select: Definition and implementation of organization-defined cryptographic uses and types in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standard is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.3.1**, **AS-2.5.1**, and **AS-2.7.1**.

## **SC-15 COLLABORATIVE COMPUTING DEVICES**

Justification to Select: Prohibiting remote activation of collaborative computing devices except with approved exceptions and providing explicit indication of use to users

physically present at the devices is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-3.2.4.

Applicable Control Enhancements: (1), (2), (3), and (4).

#### **SC-16 TRANSMISSION OF SECURITY ATTRIBUTES**

Justification to Select: Defining and associating security attributes and requirements with the information exchanged between information systems and between systems components are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-4.2.5.

Applicable Control Enhancements: (1).

#### **SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES**

Justification to Select: Issuing or obtaining public key certificates according to DoD policy and/or from an approved service provider, and managing trust stores to allow only approved trust anchors is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-2.1.15 and AS-2.5.1.

#### **SC-18 MOBILE CODE**

Justification to Select: Defining acceptable and unacceptable mobile code and mobile code technologies, establishing usage restrictions and guidance for their use, and authorizing, monitoring and controlling the use of mobile code are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-4.1.6.

Applicable Control Enhancements: (1), (2), (3), (4), and (5).

#### **SC-19 VOICE OVER INTERNET PROTOCOL**

Justification to Select: Establishing usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies, and authorizing, monitoring and controlling the use of VOIP within an information system are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique CM-5.1.6.

#### **SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**

Justification to Select: Providing additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries, and the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC 2.1.18.

Applicable Control Enhancements: (2).

#### **SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**

Justification to Select: Requesting and performing data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC 2.1.18.



## **SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**

Justification to Select: Designing information systems that collectively provide name/address resolution service for an organization to be fault-tolerance and the implementation of internal/external role separation is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC 2.1.18.

## **SC-23 SESSION AUTHENTICITY**

Justification to Select: Protection of the authenticity of communications sessions is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.2.1**, AC-1.2.2, AC-2.1.14, **AC-2.1.16** and, **AC-2.1.18**.

Applicable Control Enhancements: (1), (3), and (5).

## **SC-28 PROTECTION OF INFORMATION AT REST**

Justification to Select: Protecting the confidentiality and integrity of data at rest is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-4.3.1 and CP-2.1.2.

Applicable Control Enhancements: (1) and (2).

## **SC-32 INFORMATION SYSTEM PARTITIONING**

Justification to Select: Partitioning the information system components that reside in separate physical domains or environments based on organizational requirements is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-3.1.16**, **AS-3.6.1**, **AS-3.6.2**, and **DA-1.1.2**.

## **SC-36 DISTRIBUTED PROCESSING AND STORAGE**

Justification to Select: Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-2.1.1** and CP-2.1.3.

Applicable Control Enhancements: (1).

## **SC-37 OUT-OF-BAND CHANNELS**

Justification to Select: Employing approved out-of-band channels for the physical delivery or electronic transmission of information, information system components, or devices] to authorized individuals and systems is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **AC-1.1.2**.

Applicable Control Enhancements: (1).

## **SC-38 OPERATIONS SECURITY**

Justification to Select: Employing appropriate operations security safeguards to protect key organizational information throughout the system development life cycle is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-1.1.1** and **AS-3.3.1**.

## **SC-40 WIRELESS LINK PROTECTION**

Justification to Select: Protecting external and internal wireless links from signal parameter attacks or sources for such attacks is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.2**, **AC-1.1.6** and **AC-1.1.7**.

Applicable Control Enhancements: None.

## **SC-41 PORT AND I/O DEVICE ACCESS**

Justification to Select: Physically disabling or removing connection ports or input/output devices on designated information systems or information system components is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **BP-1.3.1**.

## **SC-43 USAGE RESTRICTIONS**

Justification to Select: Establishing usage restrictions and implementation guidance information system components based on the potential to cause damage to the information system if used maliciously, and authorizing, monitoring and controlling the use of such components within the information system are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-4.1.6**, **CM-3.1.19**, **CM-5.1.6**, and **CM-5.1.7**.

## **SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**

Justification to Select: Establishing policy and procedures for the effective implementation of selected security controls and control enhancements is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, **SM-1.2.1**, **SM-3.1.1**, **CM-5.1.2**, **CM-5.1.4**, **AS-1.1.1**, **AS-1.4.1**, and **BP-1.1.1**.

## **SI-2 FLAW REMEDIATION**

Justification to Select: Identifying information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and reporting this information to designated organizational personnel with information security responsibilities is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.7** and **CM-5.1.3**.

Applicable Control Enhancements: (1), (2), (3), (5), and (6).

### **SI-3 MALICIOUS CODE PROTECTION**

Justification to Select: Employing and appropriately configuring malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code, performing periodic scans, appropriately responding to malicious code events are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.7** and **AC-3.2.5**.

Applicable Control Enhancements: (1), (2), (4), (6), (7), (8), (9), and (10).

### **SI-4 INFORMATION SYSTEM MONITORING**

Justification to Select: Monitoring information systems to detect attacks and indicators of potential attacks and unauthorized use, and deploying and protecting monitoring devices from unauthorized access, modification, and deletion, and raising the level of information system monitoring activity are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.6**, **AC-3.2.5**, **AC-5.1.1**, **AC-5.2.1**, **AC-5.3.8**, **AC-5.3.9**, and **DA-1.2.2**.

Applicable Control Enhancements: (1), (2), (3), (4), (5), (7), (9), (10), (11), (12), (13), (14), (15), (16), (17), (18), (19), (20), (21), (22), (23), and (24).

### **SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**

Justification to Select: Receiving, generating and disseminating information system security alerts, advisories, and directives is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.7**, **AC-5.3.5**, **CM-5.1.2**, and **CM-5.1.3**.

Applicable Control Enhancements: (1).

### **SI-6 SECURITY FUNCTION VERIFICATION**

Justification to Select: Verifying the correct operation of security functions, identifying and disseminating appropriate notification of failed security verification tests, and resolving anomalies when they are discovered is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **CM-4.1.4**.

Applicable Control Enhancements: (2) and (3).

### **SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**

Justification to Select: Employing integrity verification tools to detect unauthorized changes to software, firmware, and information are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-3.2.5**, **AC-4.3.1**, **AC-5.1.1**, **AC-5.2.2**, **AC-5.3.8**, **CM-4.1.1**, **CM-4.1.2**, **CM-4.1.4**, and **AS-2.4.3**.

Applicable Control Enhancements: (1), (2), (3), (5), (6), (7), (8), (9), (10), (11), (12), (13), (14), (15), and (16).

### **SI-8 SPAM PROTECTION**

Justification to Select: Employing spam protection mechanisms at information system entry and exit points and keeping spam protection mechanisms current in accordance with organizational configuration management policy and procedures is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CM-5.1.4** and **AC-1.1.2**.

Applicable Control Enhancements: (1), (2), and (3).

## **SI-10 INFORMATION INPUT VALIDATION**

Justification to Select: Checking the validity of information inputs is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-3.2.5, **BP-1.2.1, BP-1.3.1, BP-1.4.1, BP-1.5.1, BP-1.5.2, BP-1.5.3, BP-1.6.1, BP-1.7.1, BP-1.8.1, BP-2.1.1, BP-2.3.1, BP-2.3.2, BP-4.1.1, BP-4.1.2, BP-4.1.3, BP-4.3.1, BP-4.3.2, IN-1.2.3, IN-2.1.1 and IN-2.4.1.**

Applicable Control Enhancements: (1), (2), (3), (4), and (5).

## **SI-11 ERROR HANDLING**

Justification to Select: Generating error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and revealing error messages only to personnel or roles with a need to know are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **BP-1.7.1, BP-1.8.1, BP-2.1.1, BP-2.2.2, BP-2.2.3, BP-2.3.1, BP-2.4.1, BP-2.4.2, BP-2.4.3, BP-2.4.4, BP-3.1.1, BP-3.2.1, BP-3.2.3, BP-3.3.1, BP-3.3.2, BP-3.3.3, BP-3.5.1, BP-3.5.2, BP-4.3.2, BP-4.4.4, IN-1.1.1, IN-1.2.1, IN-1.2.3, IN-2.2.1, IN-2.2.3, IN-2.4.1, IN-2.5.1, IN-2.5.2, and IN-2.5.3.**

## **SI-12 INFORMATION HANDLING AND RETENTION**

Justification to Select: Handling and retaining information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques AC-4.2.1, AC-4.2.2, AC-4.2.3, AC-4.2.4, **AC-4.2.5, AC-4.2.6, AC-5.2.7, AC-6.4.8, BP-3.1.1, BP-3.2.1, BP-3.2.2, BP-3.3.1, BP-3.3.2, BP-3.3.3, BP-3.4.1, BP-3.5.1, and BP-3.5.2.**

## **SI-13 PREDICTABLE FAILURE PREVENTION**

Justification to Select: Determining mean time to failure (MTTF) for information system components in specific environments of operation, and providing substitute information system components and a means to exchange active and standby components according to organizational criteria are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-1.2.1, CP-1.2.2, CP-2.4.5, CP-2.4.6, and CP-3.1.1.**

Applicable Control Enhancements: (1), (3), (4), and (5). Control enhancement (2) is not included as time limits on process execution without supervision is an operational requirement and not a required control for financial reporting.

## **SI-15 INFORMATION OUTPUT FILTERING**

Justification to Select: Validating information output from software programs and/or applications to verify that the information is consistent with the expected content is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques BP-3.1.1, **BP-3.2.1, BP-3.2.2, BP-3.2.3, BP-3.3.1, BP-3.3.2, BP-3.3.3, and BP-3.4.1.**

## **SI-17 FAIL-SAFE PROCEDURES**

Justification to Select: Defining and implementing fail-safe procedures when failure conditions occur is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **CP-1.3.1**, **CP-2.1.4**, CP-2.3.3, and CP-2.3.4.

## **PM-1 INFORMATION SECURITY PROGRAM PLAN**

Justification to Select: Developing, implementing and communicating an organization-wide information security program plan, periodically reviewing the plan to keep it current, and protecting it from unauthorized disclosure and modification are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-1.1.2**, SM-1.2.1, **SM-3.1.1**, **AS-1.1.1**, and AS-1.4.1.

## **PM-2 SENIOR INFORMATION SECURITY OFFICER**

Justification to Select: Appointing a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique SM-1.2.2.

## **PM-4 PLAN OF ACTION AND MILESTONES PROCESS**

Justification to Select: Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems, and reviewing plans of action and milestones to maintain consistency with the organizational risk management strategy and organization-wide priorities for risk response actions are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-6.1.1**, SM-6.1.2, and **SM-6.1.3**.

## **PM-5 INFORMATION SYSTEM INVENTORY**

Justification to Select: Developing and maintaining an inventory of its information systems are necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique **SM-1.5.1**.

## **PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE**

Justification to Select: Developing, monitoring, and reporting on the results of information security measures of performance is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique CP-2.4.9.

## **PM-8 CRITICAL INFRASTRUCTURE PLAN**

Justification to Select: Addressing information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan is necessary to satisfy FIAR guidance requirements as defined by FISCAM control technique AC-6.1.1.

## **PM-9 RISK MANAGEMENT STRATEGY**

Justification to Select: Developing and implementing a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems, and periodically reviewing and updating the risk management strategy as required, to address organizational changes are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.1.1**, **SM-5.1.1**, and **AC-6.1.1**.

## **PM-10 SECURITY AUTHORIZATION PROCESS**

Justification to Select: Managing the security state of organizational information systems and the environments in which those systems operate through security authorization processes, designating individuals to fulfill specific roles and responsibilities within the organizational risk management process, and fully integrating the security authorization processes into an organization-wide risk management program are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-1.1.1**, **AC-1.2.1**, **AC-3.1.1**, **AC-3.2.1**, **AC-4.1.1**, **AC-4.2.1**, **AC-4.3.1**, **AS-2.1.1**, **AS-2.2**, **AS-2.3.1**, **AS-2.4.1**, **AS-2.5.1**, **AS-2.6.1**, and **AS-2.7.1**.

## **PM-11 MISSION/BUSINESS PROCESS DEFINITION**

Justification to Select: Defining mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, and determining information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-1.4.1** and **AS-1.1.1**.

## **PM-14 TESTING, TRAINING, AND MONITORING**

Justification to Select: Processes for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed, executed and maintained, and for reviewing testing, training, and monitoring plans to ensure they are consistent the organizational risk management strategy and organization-wide priorities for risk response actions are necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **SM-4.3.1**, **SM-4.3.2**, **AC-1.1.2**, and **AS-1.1.1**.

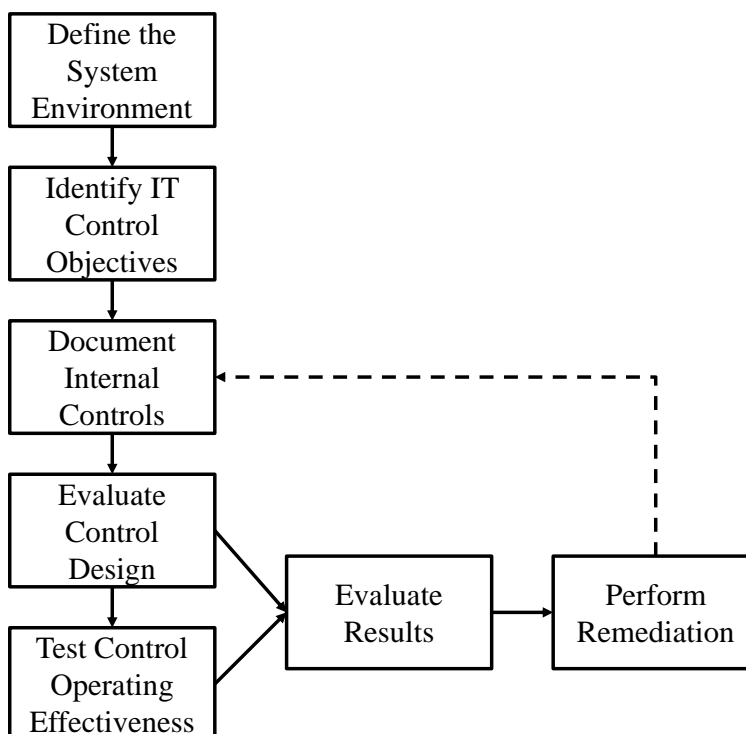
## **PM-16 THREAT AWARENESS PROGRAM**

Justification to Select: Implementing a threat awareness program that includes a cross-organization information-sharing capability is necessary to satisfy FIAR guidance requirements as defined by FISCAM control techniques **AC-5.3.6** and **AC-6.1.4**.

## Appendix 1

### Summary of FIAR Guidance Requirements for Documenting Internal Controls, Testing Control Effectiveness, and Evaluating Test Results

Information systems that affect DoD financial management, internal controls over financial reporting, and/or or are relevant for financial statement audit, as determined in Section 2: Applicability (above), should apply the FIAR Guidance across all baselines defined in CNSSI No. 1253. Figure 6 below provides a summary overview of activities to perform when evaluating the relevant internal controls over financial reporting and audit of a system. Each activity is described in further detail in sections A.1 through A.10.



**Figure 6 - Overview of activities to perform when evaluating the relevant internal controls over financial reporting and financial statement audit readiness of a system.**

In instances where the FISCAM-based FIAR Guidance and CNSSI No. 1253 control activities and techniques align, applying previously identified and documented CNSSI No. 1253 controls is encouraged, ***assuming the documentation and testing of the identified controls satisfy the FIAR Guidance (and OMB Circular A-123 Appendix A) requirements.***

In instances where the FIAR Guidance includes additional controls activities or recommended control implementation techniques incremental to those defined in CNSSI No. 1253 (and necessary to satisfy an in-scope FISCAM control objective), stakeholders must document the control, assess the design, and test the operational effectiveness of the control in accordance with the FIAR Guidance (and OMB Circular A-123 Appendix A).

## **A.1. Define the Audit Relevant Components of the System Environment**

This activity requires identifying all necessary elements of the system environment to be addressed in the audit readiness assessment, including organizations responsible for performing functions that affect internal controls over financial reporting. When completing this activity, representative information that should be documented includes the following:

- The Application Name
- The Application Owner (Organization)
- Number and Location of Production Instances (including Hosting Enclaves and Data Centers)
- Operating Systems
- Database Management Systems
- Security Management Software
- Job Scheduling Software
- Library Management Software
- Data Center and Network
- Summary of Organizational Roles and Responsibilities (such as System Owner, Hosting Organization, and User Organizations)

The system description document that is produced establishes the scope of the audit readiness assessment and is similar to the authorization boundary definition process when conducting the Risk Management Framework (RMF) activities following DoD requirements. It is important to note that all components of the system and application environment impacting internal controls over financial reporting are subject to the requirements of this Guidance.

## **A.2. Identify Information Technology Control Objectives<sup>3</sup>**

Control objectives provide a specific target against which to evaluate the effectiveness of an organization's internal controls, define the aim or purpose of the internal controls, and identify the risks that controls are intended to mitigate. Accordingly, it is necessary to identify an appropriate group of control objectives for these systems before documenting and testing specific internal controls.

### **Information Technology Control Objectives**

The GAO's FISCAM comprises two basic levels of internal controls relevant to financial information systems<sup>4</sup>:

---

<sup>3</sup> See Auditing Standard No. 5 (An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements) Section A2, American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) Number 16 (Reporting on Controls at a Service Organization) Paragraph 7, GAO/PCIE Financial Audit Manual Section 330 (Identify Control Objectives), GAO Federal Information System Controls Audit Manual pages 11 – 15 (Information System Control Objectives), and the OUSD(C) FIAR Guidance page 50.

<sup>4</sup> GAO Federal Information System Controls Audit Manual Section 1.2 (Nature of Information System Controls)



- **Information Technology General Controls (ITGCs)** - ITGCs are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect business process application programs, and ensure continued computer operations in case of unexpected interruptions. ITGCs are applied at the entity-wide level, system level, and business process (application) level. The effectiveness of general controls is a significant factor in determining the effectiveness of business process application controls.
  - Entity or System Level Information Technology General Controls (ITGCs) are pervasive across organizations, enclaves, and/or platforms and generally affect multiple applications or systems resident in the enclave or operating on a platform.
  - Application Level ITGCs are generally specific to an individual application or system (or group of applications or systems under the same management control).
- **Business Process Application Controls** - Business process application controls are directly related to individual computerized applications. They help ensure transactions are complete, accurate, valid, confidential, and available. Business process application controls include (1) programmed control techniques, such as automated edits, and (2) manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items.

It is critical to first establish control objectives applicable to the system under evaluation prior to identifying, documenting, and testing individual control activities. Each FISCAM level has multiple standard control objectives relevant to financial reporting as summarized in Table 2 below.

<b>IT General Control Objectives (applied at the Entity, Platform, <u>and</u> Application Levels)</b>	
<b>Security Management</b>	
Internal controls provide reasonable assurance that security management is effective.	
<b>Access Controls</b>	
Internal controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals.	
<b>Configuration Management</b>	
Internal controls provide reasonable assurance that changes to information system resources are authorized, and systems are configured and operated securely and as intended.	
<b>Segregation of Duties</b>	
Internal controls provide reasonable assurance that incompatible duties are effectively segregated.	
<b>Contingency Planning</b>	
Internal controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur.	

<b>Business Process Control Objectives (applied at the Application Level)</b>
<b>Completeness</b>
Internal controls provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.
<b>Accuracy</b>
Internal controls provide reasonable assurance that transactions are properly recorded, with correct amount and data, and on a timely basis (in the proper period); key data elements input for transactions are accurate; data elements are processed accurately by applications that produce reliable results; and output is accurate.
<b>Validity</b>
Internal controls provide reasonable assurance that (1) all recorded transactions actually occurred (are real), relate to the organization (are authentic), and were properly approved in accordance with management's authorization; and (2) output contains only valid data.
<b>Confidentiality</b>
Internal controls provide reasonable assurance that application data, application reports, and other output are protected against unauthorized access.
<b>Availability</b>
Internal controls provide reasonable assurance that application data, application reports, and other relevant business information are readily available to users when needed.

***Table 2 – Summary of Standard FIAR Guidance / FISCAM IT Control Objectives***

The written control objectives may be modified to reflect unique attributes of each system. Once the control objectives have been finalized, management must identify, document, and test the operating effectiveness of key controls. Key controls are those internal controls necessary to demonstrate each control objective has been satisfied.

The FIAR Guidance and FISCAM give examples of control activities and recommend control techniques that an auditor would expect to be in place to demonstrate the control objectives are satisfied. The FIAR Guidance provides additional requirements regarding appropriate documentation of internal controls, testing of internal controls, and evaluating testing results. Sections A.3 and A.4 provide a summary of the relevant FIAR Guidance for each of these activities.

### **A.3. Document Internal Controls**

Individuals responsible for evaluating the controls for each system must first understand the relevance of each FISCAM control activity and technique to the associated control objectives. A mapping of the FISCAM control activities and associated control techniques to NIST SP 800-53 control requirements is provided as Appendix 2. Individuals responsible for evaluating controls can then efficiently and effectively identify and document the **actual** control activities being performed by the organization, evaluate the design effectiveness of the controls against the control objectives, and ultimately test the operating effectiveness of the controls.

To meet the FIAR Guidance (and OMB Circular A-123 Appendix A) requirements, control documentation must include specific and accurate descriptions of the **actual** control in place for

each relevant FISCAM control technique and are typically summarized in a control matrix. The control description should identify the individual that performs the control (by job title), the frequency of the control, and evidence (hardcopy or electronic) demonstrating the control was performed as described. These elements of the control description will be factors in determining testing techniques, sample sizes, and evidence selected for testing. It is also appropriate for the control documentation to reference supporting policies and procedures related to the control and system documentation already in use within the organization. However, simply citing or referencing a DoD policy or procedure number does not constitute adequate documentation of internal controls. Similarly, simply copying and pasting the FISCAM control technique or NIST SP 800-53 / CNSS 1253 security control does not constitute adequate documentation of internal controls.

The FIAR Guidance (Section 3.D.4 – Internal Control Assessment) contains more information on documenting controls. In addition, Tables 3 and 4 provide representative examples of individual IT General, and IT Application control descriptions, respectively, that meet the requirements of this Guidance as defined by the FIAR Guidance.

Prior to testing the operating effectiveness of identified controls, determine which controls are necessary to satisfy relevant control objectives and whether the identified controls are suitably designed to satisfy the relevant control objectives. Section A.4 describes the process for evaluating the effectiveness of internal controls.

<b>FISCAM Critical Element</b>	<b>CNSSI 1253 / NIST SP 800-53 Security Control</b>	<b>FISCAM Control Activity</b>	<b>FISCAM Control Technique</b>	<b>Representative IT General Control Description</b>
AS-2: Implement effective application access controls	AC-2: Account Management	AS-2.4: Access to the application is restricted to authorized users.	AS-2.4.1: Before a user obtains a user account and password for the application, the user's level of access has been authorized by a manager and the application administrator.	Each user must submit an access request form (DD2875) to their supervisor and Information Assurance Officer (IAO) / Information System Security Manager(ISSM) for review and approval. The Information System Security Officer (ISSO) also reviews and approves the request before they provision access to the system.  Requests for certain sensitive administrative profiles would also be reviewed and approved by Core Security before they provision the access to the system.

***Table 3: Representative example description for an IT General Control***

<b>FISCAM Critical Element</b>	<b>CNSSI 1253 / NIST SP 800-53 Security Control</b>	<b>FISCAM Control Activity</b>	<b>FISCAM Control Technique</b>	<b>Representative IT Application Control Description</b>
BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	SI-9: Information Input Restrictions  SI-10: Information Input Validation  SI-11: Error Handling	BP-2.3.1: Transactions are executed in accordance with the pre-determined parameters and tolerances, specific to entity's risk management.	BP-2.3.1: Document processing and posting conditions (parameters and tolerances) are configured, including system errors and actions, if the conditions are not met.	<p>The system has 4,056 automated edit checks in place covering all material transaction types. These context sensitive edits check for multiple criteria including duplicate batches and transactions, date and period checking, and entered amounts. The system has 395 standard reports available for use in analyzing the status of transactions processed.</p> <p>The input sub-system performs many of the same edits and issues warning messages to alert users if they enter incorrect or incomplete data. The input sub-system also makes extensive use of drop-down selection lists to facilitate the entry and selection of valid input options. In the event that a user ignores input sub-system warning messages and the transaction is submitted, it would be subject to the standard system edits.</p> <p>The input sub-system also uses pre-fill technology to automatically populate certain data fields once key identifier information is entered.</p>

***Table 4: Representative example description for an IT Application Control***

#### **A.4. Evaluate Control Design**

Once the control activities associated with the individual relevant FISCAM control techniques have been identified and documented, these control activities must be evaluated to determine if they have been designed effectively. This process consists of three basic steps:

- 1) Identify those instances where no controls were documented to address the relevant FISCAM control techniques.
- 2) For those instances where controls have been identified, determine if the control (as described) clearly indicates the relevant FISCAM control technique has been addressed.

- 3) Determine if the population of identified controls, working together, satisfies the relevant FISCAM control objectives. Factors to consider when making this determination include:
  - Directness (extent control activities relate to the control objective),
  - Selectivity (impact the control has, or does not have, on the financial system),
  - Manner of execution (frequency of control activity execution and skills and experience of personnel performing the control activity), and
  - Follow-up (procedures performed when the control activity identifies an exception).

In the event the organization does not have a control in place for the system, or the identified controls are not properly designed to satisfy the control objectives, corrective action plans should be developed and completed to remediate the identified deficiencies. Additional information relating to assessing the design effectiveness of internal controls can be found in the FIAR Guidance (Section 3.D.4 – Internal Control Assessment).

There are two important outcomes of the control design assessment process:

- 1) Identification of instances where controls do not exist, are not properly designed, and remediation is necessary.
- 2) Identification of properly designed controls, necessary to satisfy the control objectives, to be tested for operating effectiveness. Only control activities which are properly designed should be tested for operating effectiveness

#### **A.5. Test Control Operating Effectiveness**

For controls that are designed effectively and are necessary to satisfy one or more control objectives, management must test the operating effectiveness of the controls over a period of time in accordance with FIAR Guidance (and OMB Circular A-123 Appendix A) requirements. This requires development and execution of test plans for the relevant control(s). This process can be broken down into the following summarized activities:

- Select an appropriate testing technique, or combination of techniques, for each control. When completing this activity, management should consider the evidence available to demonstrate the controls were performed and also reference the specific FISCAM testing techniques provided in the FIAR Guidance.
- Determine an appropriate sample size and acceptable error rate. When completing this activity, management should consider the type of control (automated versus manual) and frequency of the control. This information should be available from the documented control description and is necessary to determine an appropriate sample size.
- Identify an appropriate population from which the control testing samples will be selected. It is important that the population represents all activity performed for the sample period and facilitates testing of the identified controls.
- Identify the types of evidence that will be required to provide evidence the controls are operating effectively during the testing process. As noted earlier, the control description should identify the relevant and available evidence to be requested for testing.

- Create a test plan that captures the attributes of the test (described above) along with the relevant control description and additional instructions as needed. Section 3.D.4 (Internal Control Assessment) of the FIAR Guidance provides additional instructions for creating test plans and an example template.
- Perform the test as specified in the plan, record the results, and evaluate the results for each individual control. It is critical that a supportable conclusion on the operating effectiveness of the control is documented based solely on the test results.
- Conclude if the identified controls, when aggregated, are operating effectively and satisfy the control objectives.
- Develop corrective action plans for controls that are not operating effectively and are necessary for satisfying the control objectives. Note the corrective actions ***must be implemented*** for key controls to meet FIAR Guidance requirements.

Once the tests of control activities are complete, the results must be documented. This documentation provides support for the entity's assertion that the system is audit ready and the Department's annual Statement of Assurance. These assertions may be reviewed by the independent auditor and possibly by the DoD IG, GAO, or OMB. Thus, the testing should be sufficiently documented to allow an independent person to understand and re-perform the test. The detailed testing documentation should describe the specific items tested (e.g., the title and date of reports, document numbers, system change request numbers, etc.), identify the person who performed the testing, and describe the test results.

Summary guidance for testing control operating effectiveness is provided in subsequent sections, and detailed instructions and templates are provided in the FIAR Guidance. A mapping of the FISCAM control activities and associated control techniques to NIST SP 800-53 control requirements is provided as Appendix 2. To minimize duplication of efforts, management is encouraged to identify related assessment activities and apply the results from those related initiatives ***to the extent they meet the documentation and testing requirements established in the FIAR Guidance*** (and OMB Circular A-123 Appendix A). Representative assessment activities include:

- FMFIA / FFMIA / MICP Self-Assessments
- FISMA Self-Assessments
- Internal Audits
- DoD IG and GAO Audits

Tables 5 and 6 provide representative examples of summary IT General, and IT Application control testing results assessments, respectively, that meet the requirements of this Guidance as defined by the FIAR Guidance. As indicated earlier, detailed test plans identifying the specific sample items selected and attributes tested would also be required. More information around testing the effectiveness of internal and security controls is in the FIAR Guidance (Section 3.D.4 – Internal Control Assessment).

FISCAM Critical Element	FISCAM Control Activity	FISCAM Control Technique	Control Test of Effectiveness	Result of Operational Effectiveness Assessment
AS-2: Implement effective application access controls	AS-2.4: Access to the application is restricted to authorized users.	AS-2.4.1: Before a user obtains a user account and password for the application, the user's level of access has been authorized by a manager and the application administrator.	Select a sample of application users and inspect the approvals from the manager and application administrator.	<p><b><u>Test Summary</u></b> Inquired of management and inspected the System Security Plan, the Information Assurance Officers Manual, and the Guide for System Administrative Information Assurance Officers (IAOs) to determine whether an access request and approval process has been established for the system.</p> <p>A sample of 45 users from instance one and 45 users from instance two were selected and the access request forms (DD 2875) were inspected.</p> <p><b><u>Result</u></b></p> <ul style="list-style-type: none"> <li>• Of the 90 users selected, 3 access request forms could not be located.</li> <li>• For the 87 access request forms that could be located, 2 were missing signature pages.</li> <li>• For the 87 access request forms that could be located, 1 was missing and information owner signature.</li> <li>• For the 87 access request forms that could be located, there were 25 instances where the user access rights could not be reconciled to the information on the access request form.</li> </ul> <p><b><u>Conclusion</u></b> Exceptions noted - The control is <b>NOT</b> operating effectively.</p>

***Table 5 - Representative example for an IT General Control operating effectiveness assessment for a control that is not operating effectively***

<b>FISCAM Critical Element</b>	<b>FISCAM Control Activity</b>	<b>FISCAM Control Technique</b>	<b>Control Test of Effectiveness</b>	<b>Result of Operational Effectiveness Assessment</b>
BP-2: Transaction Data Processing is complete, accurate, valid, and confidential.	BP-2.3.1: Transactions are executed in accordance with the pre- determined parameters and tolerances, specific to entity's risk management.	BP-2.3.1: Document processing and posting conditions (parameters and tolerances) are configured, including system errors and actions, if the conditions are not met.	Inspect configuration of parameters and tolerances levels defined by the entity to identify whether the application processes the data with warning or rejects the data, if the conditions are not met.	<p><b><u>Test</u></b> Identified a sample of system edit checks necessary to address in-scope control objectives and created a set of test transactions designed to fail the edit checks. Entered the sample transaction in a test environment and observed the results.</p> <p><b><u>Result</u></b> Observed as a the sample test transactions were entered into the input subsystem and noted certain fields were required, the system prepopulated certain fields based on entered values, and the warning messages were issued when inaccurate data was entered.</p> <p>Observed as data from the input subsystem was batched and uploaded to the system test region noting expected errors were reported on the Daily Transaction Register and not accepted for processing by the system.</p> <p><b><u>Conclusion</u></b> No exceptions noted – The control is operating effectively.</p>

***Table 6 - Representative example for an IT Application Control operating effectiveness assessment for a control that is operating effectively***



### A.5.1 Testing Techniques

Testing techniques can be classified into four basic types: inquiry, observation, inspection, and re-performance. Combining two or more of these test techniques provides greater assurance than using only one testing technique. The types of testing techniques are described in Table 7.

Testing Technique	Description
Inquiry	Conducted by making either verbal or written inquiries of entity personnel involved in the execution of specific control activities to determine what they do or how they perform a specific control activity. The least reliable type of test.
Observation	Conducted by observing entity personnel performing control activities in the normal course of their duties. Provides a higher degree of reliability than inquiry and may be an acceptable technique for assessing automated controls.
Inspection	Examination of evidence is often used to determine whether manual control activities are being performed. Inspections are conducted by examining documents and records for evidence (such as the existence of initials or signatures) that a control activity was applied to those documents and records.
Re-performance	Independently repeating the control in place.

*Table 7 - Summary of common internal control testing techniques.*

The extent of testing of a control activity will vary depending on a variety of factors, including whether a control activity is automated or manual.

#### Testing of Automated Control Activities

For an automated control activity, and assuming ITGCs have been tested and found to be operating effectively, the number of items tested can be minimal (one to a few items). It is management's responsibility to ensure the automated control activities are working as designed and that there are alternative methods that may be used to accomplish this objective. Alternative methods may include inspecting configuration settings, reviewing program code, performing walkthroughs of transactions, and observing and confirming that all relevant transaction types and error conditions are covered.

#### Testing of Manual Control Activities

Tests of manual control activities (control activities performed manually, not by computer) should include a mix of inquiry, observation, examination, or re-performance. Inquiry alone does **not** provide sufficient evidence to support the control activity's operating effectiveness. Effective testing generally requires examining the application of a control activity at a particular location many times (referred to as sampling). Although

the entity may find nothing amiss in the samples (resulting in a conclusion that a control is operating effectively), sampling brings the inherent risk that the control is not operating effectively at *all* times. Sampling risk should be minimized by selecting a sufficient number of items to test (e.g., using either statistical or judgmental sampling). Sampling risk increases with the frequency of the control's execution. Section A.5.2 provides sampling guidance.

The time period of time over which application or system stakeholders test control activities must be sufficient to determine operating effectiveness as of the report date of the reviews, (i.e., audit readiness assertion when applicable or annual statement of assurance). Testing should be performed in increments throughout the period being reviewed. The period tested must be sufficient to enable stakeholders to obtain adequate evidence about the control activities' operating effectiveness. At a minimum, the entity must have performed enough tests of control activities to meet the minimum sample sizes noted in Table 9 (e.g., for a monthly control, at least three months be tested for the entity to be able to conclude on the operating effectiveness of its control activity).

Section A.5.2 provides details around sampling methodologies appropriate for internal controls testing. All control parameters and thresholds (i.e. account lock threshold) shall remain consistent with DoD and CNSS guidance.

## A.5.2 Sample Sizes and Acceptable Error Rates

The FIAR Guidance (Section 3.D.4 – Internal Control Assessment).incorporated recommendations for sample sizes and the acceptable number of deviations from The CFO Council, Implementation Guide for OMB Circular A-123 (Appendix A). However, for larger sample sizes, the Department determined that a higher number of deviations will be permitted to support audit readiness assertions. Management should *not* interpret this to mean corrective actions are unnecessary for identified testing exceptions. The sample sizes and acceptable number of deviations are summarized in Table 8.

Frequency	Population Size	Total Sample Size	Acceptable Number of Deviations/Tolerable Misstatement (CFO Council)*	Acceptable Number of Deviations/Tolerable Misstatement (Audit Readiness Guidance)
Annual	1	1	0	0
Quarterly	4	2	0	0
Monthly	12	3	0	0
Weekly	52	10	0	1
Daily	250	30	0	3
Multiple Times per day	Over 250	45	0	5

\*Represent number of deviations to most likely be used by an auditor when performing an audit.

**Table 8 - Frequency of Control Activity Determines Sample Size and Acceptable Error Rates**

Management must accept the inherent risks of sampling and understand that testing under a financial statement audit will be even more rigorous and allow fewer deviations. Furthermore, entities must document the justification of the sample size used for testing if it differs from the FIAR Guidance (ex., the number of occurrences of the activity was less than the recommended sample size).

Further information around sampling techniques and the consideration of location when selecting a sample can be found in the FIAR Guidance (Section 3.D.4 – Internal Control Assessment)..

## **A.6 Guidance**

### **A.6.1 Coordination with Other Compliance Requirements**

Assessment activities completed in accordance with the requirements of this Guidance should be integrated into existing organizational processes, such as annual security assessments for FISMA or continuous monitoring strategies for assessment and authorization of the system. Outputs from assessment activities should include a comprehensive and descriptive listing of internal and security controls and may be used to meet FIAR, OMB Circular A-123, MICP, or FISMA deliverables.

### **A.6.2 Controls Performed by Other/External Organizations**

When defining the system environment and documenting internal controls, management may identify one or more organizations that have responsibility for performing controls relevant to the system. These are commonly referred to as service organizations and a frequently encountered example is a third party system hosting or data center service provider such as The Defense Information Systems Agency.

When a service organization is performing audit relevant controls, management still retains overall responsibility for obtaining assurance that the necessary controls have been established, are operating effectively, and satisfy the control objectives. Some options for obtaining this assurance follow:

- The organization responsible for the system documents and tests the service organization's controls in accordance with the FIAR Guidance.
- The service organization documents and tests the controls within their organization, in accordance with the FIAR Guidance, and provides the results to the organization responsible for the system.
- As available, the organization responsible for the system obtains and evaluates a Service Auditor's Report prepared under Statement on Standards for Attestation Engagements Number 16 (SSAE No. 16)<sup>5</sup> that provides an opinion on the design and operating effectiveness of internal controls at the service organization.

Addition information may be found in the FIAR Guidance (Sections 4.A.2 – Consideration of Service Providers and 4.B Service Provider Methodology).

---

<sup>5</sup> American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) Number 16 (Reporting on Controls at a Service Organization)

### A.6.3 Systems Under Development

A phased approach for documenting and testing the effectiveness of internal controls may be necessary for systems still under development. A control design assessment must be completed before the “Execution – Engineering Development Phase” of the DoD Business Capability Lifecycle (and prior to Milestone C approval). During this design assessment, management must complete, at a minimum, the following for the planned system capability:

- Document the relevant IT General controls.
- Document the programmed and configured IT Application controls.
- Evaluate the design of the identified controls.
- Identify and complete necessary corrective actions.
- Document a conclusion regarding the *design* effectiveness of internal controls.

Once the “BCL Execution – Limited Fielding” phase has been initiated, but prior to full deployment, management must then complete the following to evaluate the design and operating effectiveness of internal controls for the planned system capability:

- Update documentation of the relevant IT General controls and programmed (or configured) IT Application controls (as needed).
- Document the manual IT Application controls relevant to the capability.
- Evaluate the design of updated or additional controls.
- Design and complete tests of control *operating* effectiveness.
- Identify and complete necessary corrective actions.
- Document the conclusion regarding the *design and operating* effectiveness of internal controls.

### A.7 Regulatory and Statutory Controls

Federal agencies are required to maintain a financial management system that complies with applicable regulations and statutes. The Federal Financial Management Improvement Act (FFMIA) of 1996 requires financial management systems to substantially comply with financial management system requirements, Federal accounting standards, and record transactions in alignment with the U.S. Government Standard General Ledger. To meet compliance requirements as defined by FFMIA, systems following this Guidance should ensure they have integrated DFAS 7900.4-M and OMB Circular A-123 (Appendix D) guidance and controls into system configuration and baselines.

Per the Federal Managers’ Financial Integrity Act (FMFIA) of 1982, management must assess the effectiveness of internal control over financial reporting and compliance with financial related laws and regulations on an *annual* basis.

## A.8 Tailoring Considerations

Stakeholders following the requirements of this Guidance should take into consideration other work performed around internal and security controls within the application's IT environment (e.g. OMB Circular A-123 reviews, FISMA reviews). Appendix 2 provides a detailed mapping of NIST SP 800-53, Rev 4 to individual FISCAM control techniques.

Where possible and appropriate (i.e., the FIAR Guidance requirements are met), the organization may apply results from alternate testing and tailor FISCAM testing accordingly. The organization's management is ultimately responsible for accepting the risk in using testing results and should take this risk into account when determining whether to use alternate sources of testing. Additionally, if the organization performing FISCAM testing makes a risk-based decision to exclude specific control techniques from testing, the justification and risk acceptance should be documented and approved by management.

Examples of when it may be appropriate to exclude testing (or reduce sample sizes) in a given year could include the following:

- Automated system edit checks have been tested successfully for multiple consecutive years and management has successfully tested system configuration and change management controls in the current year. In this circumstance, management may conclude there is a low risk that the automated edit checks were inappropriately modified and defer testing to the following year.
- Management has successfully tested system user access approvals for multiple consecutive years, and there have been no changes to applicable policies, procedures, or security responsibility assignments. In this circumstance, management may conclude there is a low risk of unapproved user access and reduce the sample size from 45 to 30 items.

In determining the relative priority and timing of controls documentation and testing, the effectiveness of general controls is a significant factor in management's assessment of the effectiveness of business process application controls. Furthermore, without effective general controls, business process application controls can generally be rendered ineffective by circumvention or modification.

## A.9 Duration

Evaluation of an information system's internal control should be performed in accordance and conjunction with applicable laws, regulations, and reporting requirements. The FMFIA of 1982, OMB Circular A-123, and the DoD MICP require management to perform a review of the internal controls over financial reporting on an **annual** basis. The Federal Information Security Management Act of 2002 requires organizations to conduct assessments of security controls at a frequency commensurate with risk but no less than **annually**. As DoD implements a more dynamic, continual monitoring process in line with NIST SP 800-137 and DoDI 8510.01, the controls, or a subset of controls, associated with financial management systems should be evaluated no less than **annually**.

## A.10 Definitions

OMB Circular A-123 (Appendix D) (and the predecessor OMB Circular A-127), FISCAM, and the FIAR Guidance provide definitions for systems associated with the financial management processes of an agency.

Financial / Accounting Event	<b>Any</b> activity having financial consequences to the Federal government related to the receipt of appropriations or other financial resources; acquisition of goods or services; payments or collections; recognition of guarantees, benefits to be provided, or other potential liabilities; distribution of grants; or other reportable financial activities.
Financial Management System	A <b>financial management system</b> includes an agency's overall financial operation, reflecting the people, processes, and technology to capture, classify, summarize, and report data in a meaningful manner to support business decisions. It includes hardware, applications and system software, personnel, procedures, data, and reporting functions. The financial management system <b>can be fully integrated with other management information systems (i.e., mixed systems)</b> where transactions automatically flow into an accounting general ledger. The financial management system could also include manual processes to post transactions from other management systems into the accounting general ledger.
Financial System	<p>The <b>financial system</b> is an information system or set of applications that the accounting portion of the financial management system maintains summary or detailed transactions resulting from budgetary and proprietary financial activity. The financial system encompasses processes and records that:</p> <ul style="list-style-type: none"><li>• Identify and record all valid transactions;</li><li>• Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting;</li><li>• Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements; and</li><li>• Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.</li></ul>
IT Application Controls	IT Business process application level controls, commonly referred to as application-level controls or <b>application controls</b> , are those controls over the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

Internal Control	<p>An integral component of an organization's management that provides reasonable assurance that the following objectives have been met:</p> <ul style="list-style-type: none"> <li>• effectiveness and efficiency of operations,</li> <li>• reliability of financial reporting, and</li> <li>• compliance with applicable laws and regulations.</li> </ul>
IT General Controls	<p><b>IT General controls</b> are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entity-wide, system, and business process application levels.</p>
Materiality	<p><b>Materiality</b> is the magnitude of an item's omission or misstatement in a financial statement that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item.</p>
Mixed System	<p>A <b>mixed system</b> is a hybrid of financial and non-financial portions of the overall financial management system. The following are examples of mixed systems: payment and invoice systems, procurement systems, receivable systems, loan systems, grants systems, payroll systems, budget formulation systems, billing systems, property management systems, travel systems, or <b>other</b> mission operational systems that impact a financial system.</p>

## Appendix 2

### FISCAM to NIST SP 800-53 Mapping

#### Summary Mapping of FISCAM Control Techniques to NIST SP 800-53 Controls and Control Enhancements

NIST SP 800-53 to FISCAM Overview Mapping	
NIST 800-53 Control Number	FISCAM Control Technique
AC-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> AC-2.1.2 <b>AS-1.1.1</b> <b>AS-1.1.2</b> <b>AS-1.3.1</b> <b>AS-1.3.2</b> AS-1.4.1 <b>AS-2.6.1</b> <b>AS-2.7.1</b>
AC-2	AS-3.1 AS-3.2.3 <b>AC-3.1.1</b> <b>AC-4.1.2</b> <b>SD-1.1.7</b> SD-1.3.3 SD-2.2.1 <b>SD-2.2.2</b> <b>SD-2.2.3</b> <b>SD-2.2.5</b> <b>AS-1.1.2</b> <b>AS-1.3.1</b> <b>AS-2.4.1</b> <b>AS-2.4.2</b> <b>AS-2.4.3</b> <b>AS-2.5.1</b> <b>AS-2.6.2</b> <b>AS-2.6.3</b> <b>AS-2.6.4</b> <b>AS-2.6.5</b> <b>AS-3.8.1</b> <b>AS-4.4.1</b> BP-3.5.1 BP-3.5.2 BP-4.7.1 <b>DA-1.1.3</b> <b>DA-1.3.2</b>
AC-2 (1)	<b>AC-3.1.4</b> <b>AC-3.1.5</b>
AC-2 (2)	<b>AC-3.1.10</b>
AC-2 (3)	<b>AC-3.1.8</b>



## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
AC-2 (4)	<b>AC-3.1.2</b> <b>AC-5.2.3</b>
AC-2 (5)	<b>AS-2.3.2</b>
AC-2 (7)	<b>AC-3.1.2</b>
AC-2 (9)	<b>AS-4.1.1</b> <b>AC-4.1.2</b> <b>AC-4.1.3</b> <b>AC-4.1.4</b> <b>AC-4.1.5</b> AC-4.1.6 AC-4.1.7 <b>AC-4.1.8</b> <b>AC-4.1.9</b> AC-4.1.10
AC-2 (10)	<b>AC-2.1.9</b> <b>AC-3.1.8</b>
AC-2 (11)	<b>AC-1.1.7</b> AC-1.2.3
AC-2 (12)	<b>AC-5.1.1</b> <b>AC-5.3.1</b> <b>AS-2.10.1</b>
AC-2 (13)	<b>AC-3.1.8</b> <b>AC-5.1.1</b>
AC-3	<b>AC-3.1.2</b> <b>AC-4.1.3</b> AC-4.1.7 <b>SD-1.1.7</b> SD-1.3.3 <b>AS-2.1.1</b> <b>AS-2.4.3</b> <b>AS-2.7.1</b> <b>AS-3.8.1</b> <b>AS-4.2.1</b> <b>AS-4.3.1</b>
AC-3 (2)	AC-2.1.4 <b>AC-2.1.16</b>
AC-3 (3)	<b>AC-3.1.2</b>
AC-3 (4)	<b>AC-3.1.2</b>
AC-3 (5)	<b>AS-2.7.1</b>
AC-3 (7)	<b>AS-3.8.1</b>
AC-3 (8)	<b>AS-2.4.2</b>
AC-3 (9)	<b>IN-1.2.1</b> AC-4.2.1 AC-4.2.2 AC-4.2.3 AC-4.2.4 <b>AC-4.2.5</b> AC-4.2.6
AC-3 (10)	<b>AS-1.1.2</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
AC-4	<b>AC-1.1.1</b> <b>AC-1.1.2</b> AC-5.3.9 <b>AS-2.1.1</b> <b>BP-2.5.1</b> <b>BP-2.6.1</b> <b>BP-2.7.2</b> BP-2.8.1 <b>BP-2.9.1</b> <b>IN-2.2.2</b>
AC-4 (1)	<b>AS-2.1.1</b> <b>AS-3.8.1</b>
AC-4 (2)	<b>IN-2.1.1</b> <b>IN-2.3.1</b>
AC-4 (3)	<b>AC-1.1.1</b> <b>AC-1.1.2</b>
AC-4 (7)	<b>AC-1.1.1</b> <b>AC-1.1.2</b>
AC-4 (8)	<b>IN-1.2.1</b> <b>BP-1.5.1</b>
AC-4 (9)	<b>BP-3.3.1</b> <b>BP-3.3.2</b>
AC-4 (10)	<b>IN-2.1.1</b> <b>IN-2.2.1</b>
AC-4 (11)	<b>BP-1.5.1</b>
AC-4 (12)	<b>IN-2.3.1</b>
AC-4 (17)	<b>IN-2.1.1</b>
AC-4 (20)	<b>IN-2.1.1</b> <b>IN-2.3.1</b>
AC-4 (21)	AC-1.1.4 <b>IN-2.2.2</b>
AC-4 (22)	<b>SM-3.1.1</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
AC-5	<b>CM-3.1.16</b> <b>SD-1.1.1</b> <b>SD-1.1.2</b> <b>SD-1.1.3</b> <b>SD-1.1.4</b> <b>SD-1.1.5</b> SD-1.1.6 SD-1.3.3 SD-2.1.1 SD-2.1.2 SD-2.1.3 SD-2.2.1 <b>SD-2.2.2</b> <b>SD-2.2.3</b> SD-2.2.4 <b>SD-2.2.5</b> <b>AS-1.1.3</b> <b>AS-1.3.2</b> <b>AS-2.4.3</b> <b>AS-2.6.1</b> <b>AS-2.6.2</b> <b>AS-2.6.3</b> <b>AS-2.6.4</b> <b>AS-2.6.6</b> <b>AS-3.10.1</b> <b>AS-3.11.1</b> <b>AS-4.1.1</b> <b>AS-4.1.2</b> <b>AS-4.2.1</b> <b>AS-4.3.1</b> <b>AS-4.4.1</b> <b>AS-4.4.2</b> <b>AS-4.4.3</b> <b>AS-4.5.1</b> <b>AS-4.5.2</b> <b>AS-4.5.3</b> <b>BP-3.2.3</b> <b>BP-3.5.2</b> <b>BP-4.4.3</b> <b>DA-1.1.3</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
AC-6	<b>AC-3.1.5</b> <b>AC-3.1.6</b> <b>AC-3.1.9</b> <b>AC-3.2.1</b> AC-3.2.2 AC-3.2.3 AC-3.2.5 <b>AC-4.1.1</b> <b>AS-1.1.2</b> <b>AS-1.1.3</b> <b>AS-1.3.2</b> <b>AS-2.4.3</b> <b>AS-2.6.1</b> <b>AS-2.6.2</b> <b>AS-2.6.3</b> <b>AS-2.6.4</b> <b>AS-2.6.6</b> <b>AS-3.10.1</b> <b>AS-3.11.1</b> <b>AS-4.1.1</b> <b>AS-4.1.2</b> <b>AS-4.2.1</b> <b>AS-4.3.1</b> <b>AS-4.4.1</b> <b>AS-4.4.2</b> <b>AS-4.4.3</b> <b>AS-4.5.1</b> <b>AS-4.5.2</b> <b>AS-4.5.3</b> <b>BP-3.2.3</b> BP-3.5.1 BP-3.5.2 <b>DA-1.1.3</b>
AC-6 (1)	<b>AS-2.6.2</b> <b>AC-3.1.1</b>
AC-6 (2)	<b>AS-4.3.1</b>
AC-6 (3)	<b>BP-1.3.1</b> <b>AC-6.1.2</b>
AC-6 (4)	None
AC-6 (5)	<b>AS-2.6.6</b>
AC-6 (6)	<b>SM-7.1.1</b>
AC-6 (7)	<b>AS-2.6.4</b> <b>AC-3.1.5</b>
AC-6 (9)	<b>AS-2.8.1</b>
AC-6 (10)	<b>AS-4.3.1</b>
AC-7	<b>AC-2.1.7</b> <b>AS-2.3.2</b>
AC-8	AC-1.2.3
AC-9	AC-1.2.3
AC-9 (1)	AC-2.1.2

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
	<b>AC-2.1.3</b> <b>AC-2.1.7</b> <b>AC-3.1.3</b> <b>AC-3.1.4</b>
AC-10	AC-2.1.14 AS-2.3.4
AC-11	<b>AC-1.2.1</b> <b>AS-2.3.2</b>
AC-11 (1)	<b>AC-1.2.1</b>
AC-12	AC-1.2.2 <b>AS-2.3.2</b>
AC-12 (1)	None
AC-14	<b>AC-2.1.1</b>
AC-16	<b>AC-2.1.15</b> <b>AC-4.1.1</b> AC-4.2.2
AC-16 (1)	None
AC-16 (2)	<b>AS-2.6.2</b> <b>AC-3.1.1</b>
AC-16 (3)	None
AC-16 (4)	<b>AS-2.6.2</b> <b>AC-3.1.1</b>
AC-16 (10)	<b>AS-2.6.2</b> <b>AC-3.1.1</b>
AC-17	AC-1.1.4 AC-1.1.5 AC-1.1.6 <b>AC-1.1.7</b> <b>AC-4.1.3</b> AC-4.3.1 AC-4.3.2
AC-17 (1)	<b>AC-2.1.3</b> <b>AC-4.1.2</b>
AC-17 (2)	<b>AC-1.1.2</b> AC-1.1.5
AC-17 (3)	AC-1.1.4 AC-1.1.5 AC-1.1.6
AC-17 (4)	<b>AC-1.1.7</b>
AC-17 (6)	<b>AC-1.1.2</b> AC-1.1.6
AC-18	AC-1.1.6 <b>AC-1.1.7</b> AC-4.3.2
AC-18 (1)	AC-1.1.6
AC-18 (3)	<b>AC-1.1.1</b> <b>AC-1.1.2</b>
AC-18 (4)	<b>AC-1.1.7</b>
AC-18 (5)	AC-1.1.6

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
AC-19	<b>AC-1.1.7</b> AC-4.3.2
AC-19 (5)	None
AC-20	<b>SM-7.1.1</b>
AC-20 (1)	<b>BP-1.2.1</b>
AC-20 (2)	<b>AC-1.1.7</b>
AC-20 (3)	<b>AC-1.1.7</b>
AC-20 (4)	None
AC-21	<b>SM-1.1.1</b> <b>AC-3.1.1</b> through <b>AC-3.1.10</b> <b>AC-3.2.1</b> through AC-3.2.5 <b>AS-1.1.1</b>
AC-22	<b>AS-2.5.1</b> AC-3.2.5
AC-23	<b>DA-1.2.1</b> <b>DA-1.2.2</b>
AC-24	<b>AC-3.1.1</b> through <b>AC-3.1.10</b>
AC-24 (1)	<b>AC-2.1.15</b> <b>AC-2.1.18</b>
AC-25	<b>AC-3.2.1</b> through AC-3.2.5
AT-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>SM-4.1.1</b> SM-4.1.2 <b>SM-7.1.1</b> <b>AS-1.1.1</b> AS-1.4.1 AS-1.4.2
AT-2	<b>SM-4.1.1</b> SM-4.1.2 <b>AC-6.1.5</b> SD-1.3.2 AS-1.4.2
AT-2 (1)	AC-6.1.7 <b>AC-6.1.5</b>
AT-2 (2)	<b>AC-1.1.2</b>
AT-3	<b>SM-4.1.1</b> SM-4.1.2 SD-1.3.2 CP-2.3.1 CP-2.3.2 AS-1.4.2
AT-3 (1)	<b>AC-6.4.3</b> CP-2.2.9
AT-3 (2)	AC-6.1.1 <b>AC-6.1.2</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
AT-3 (3)	<b>AC-1.1.2</b>
AT-3 (4)	<b>CM-1.1.1</b>
AT-4	<b>SM-4.1.1</b> <b>SM-4.3.2</b> <b>AC-6.1.5</b>
AU-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AS-1.1.1</b> AS-1.4.1 <b>AS-2.8.1</b> <b>BP-2.9.2</b>
AU-2	AC-5.2.2 <b>AC-5.2.3</b> <b>AS-2.8.1</b> <b>BP-2.2.1</b> <b>BP-2.2.2</b> <b>BP-2.2.3</b>
AU-2 (3)	AC-5.2.2
AU-3	<b>AC-5.2.4</b> <b>AS-2.9.1</b> <b>BP-2.2.1</b> <b>BP-2.2.2</b> <b>BP-2.2.3</b> <b>BP-2.9.2</b>
AU-4	<b>AC-5.2.5</b>
AU-4 (1)	None
AU-5	<b>AC-5.2.5</b>
AU-5 (1)	<b>AC-5.2.5</b>
AU-5 (2)	<b>DA-1.2.2</b>
AU-6	<b>AC-5.2.6</b> SD-2.2.1 <b>SD-2.2.3</b> <b>SD-2.2.5</b> <b>AS-2.9.1</b> <b>AS-2.10.1</b> <b>BP-2.9.2</b> <b>BP-2.9.3</b> <b>BP-2.9.4</b> <b>IN-2.4.1</b> <b>IN-2.5.3</b> <b>DA-1.2.1</b>
AU-6 (1)	None
AU-6 (7)	<b>AC-3.1.1</b> <b>AC-3.1.6</b>
AU-6 (10)	None

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
AU-7	<b>AC-5.2.4</b> <b>AC-5.2.6</b> <b>AS-2.10.1</b>
AU-7 (1)	<b>AC-5.2.4</b>
AU-8	<b>AC-5.2.4</b>
AU-8 (1)	<b>AC-5.2.4</b>
AU-9	AC-4.3.1 <b>AC-5.2.6</b>
AU-9 (2)	<b>AC-5.2.7</b> <b>CP-2.1.1</b> CP-2.1.3
AU-9 (4)	<b>AC-5.2.6</b>
AU-9 (6)	<b>AC-5.2.6</b>
AU-10	<b>AC-2.1.1</b> <b>AC-2.1.15</b>
AU-10 (1)	<b>AC-5.2.4</b> <b>DA-1.2.1</b>
AU-10 (2)	None
AU-10 (3)	None
AU-10 (4)	None
AU-11	<b>AC-5.2.7</b>
AU-12	<b>AC-5.2.3</b>
AU-12 (3)	<b>AC-5.2.6</b>
CA-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-1.4.1</b> <b>SM-1.4.2</b> <b>SM-2.1.1</b> <b>SM-3.1.1</b> <b>SM-5.1.1</b> <b>AS-1.1.1</b> AS-1.4.1 AS-1.5.1 <b>AS-1.5.2</b> AS-1.5.3



## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
CA-2	<b>SM-2.1.3</b> <b>SM-2.1.4</b> SM-2.1.6 <b>SM-5.1.1</b> SM-5.1.4 SM-5.1.5 SM-5.1.6 SM-5.1.7 AC-6.5.4 CP-2.2.9 AS-1.5.1 <b>AS-1.5.2</b> AS-1.5.3
CA-2 (1)	AC-6.1.7
CA-2 (2)	<b>AC-1.1.2</b>
CA-2 (3)	None
CA-3	<b>AC-1.1.1</b> <b>AC-1.1.2</b> <b>IN-1.1.1</b> <b>IN-1.2.1</b> <b>IN-2.1.1</b> <b>IN-2.2.1</b> <b>DA-1.1.1</b> <b>DA-1.3.2</b>
CA-3 (1)	None
CA-3 (3)	None
CA-3 (4)	AC-1.1.4 AC-3.2.5
CA-3 (5)	<b>IN-2.1.1</b>
CA-5	<b>SM-6.1.1</b> SM-6.1.2 <b>SM-6.1.3</b> <b>AS-1.6.1</b> <b>AS-1.6.2</b> <b>AS-1.6.3</b> <b>AS-1.6.4</b>
CA-6	<b>SM-2.1.4</b> SM-2.1.6
CA-7	SM-2.1.6 <b>SM-5.1.1</b> <b>AS-1.6.4</b> <b>AS-2.8.1</b> <b>IN-2.2.3</b> <b>DA-1.2.1</b> <b>DA-1.2.2</b>
CA-7 (1)	SM-5.1.6
CA-8	<b>SM-2.1.3</b> <b>AS-1.1.1</b> <b>AS-1.5.2</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
CA-8 (1)	None
CA-9	<b>AC-1.1.1</b> <b>IN-2.1.1</b>
CA-9 (1)	<b>IN-1.1.1</b>
CM-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>CM-1.1.1</b> <b>CM-2.1.1</b> <b>CM-3.1.1</b> <b>CM-4.1.3</b> <b>CM-6.1.1</b> <b>CM-6.2.1</b> <b>AS-1.1.1</b> AS-1.4.1 <b>AS-3.1.1</b> <b>AS-3.3.1</b> <b>BP-4.2.1</b>
CM-2	<b>CM-2.1.1</b> <b>CM-2.1.3</b> <b>CM-4.1.1</b> <b>CM-4.1.2</b> AS-3.2.1
CM-2 (1)	<b>CM-4.1.1</b> <b>AS-3.12.1</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
CM-3	AC-4.3.1 <b>CM-3.1.2</b> CM-3.1.3 <b>CM-3.1.4</b> <b>CM-3.1.13</b> <b>CM-3.1.14</b> <b>CM-3.1.15</b> CM-3.1.18 <b>CM-6.1.1</b> <b>CM-6.2.1</b> <b>AS-3.4.1</b> <b>AS-3.4.2</b> <b>AS-3.5.1</b> <b>AS-3.5.2</b> <b>AS-3.5.3</b> <b>AS-3.5.4</b> <b>AS-3.5.5</b> <b>AS-3.5.6</b> <b>AS-3.5.7</b> <b>AS-3.5.8</b> AS-3.5.9 <b>AS-3.6.1</b> <b>AS-3.7.1</b> <b>AS-3.9.1</b> <b>AS-3.12.1</b> <b>AS-3.14.1</b> <b>BP-4.2.2</b> <b>BP-4.2.3</b> <b>BP-4.4.1</b> <b>BP-4.4.2</b> <b>BP-4.4.4</b> <b>BP-4.5.1</b> <b>BP-4.6.1</b> <b>BP-4.6.2</b> <b>IN-1.2.2</b> <b>IN-2.2.2</b>
CM-3 (2)	<b>CM-3.1.8</b> <b>CM-3.1.15</b>
CM-3 (4)	<b>CM-1.1.1</b> <b>CM-3.1.7</b>
CM-3 (6)	<b>AC-2.1.13</b> <b>AC-2.1.16</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
CM-4	<b>CM-3.1.5</b> <b>CM-3.1.6</b> <b>CM-3.1.7</b> <b>CM-3.1.8</b> <b>CM-3.1.9</b> CM-3.1.10 <b>CM-3.1.11</b> <b>CM-3.1.12</b> <b>CM-4.1.4</b> <b>AS-3.5.1</b> <b>AS-3.5.2</b> <b>AS-3.5.3</b> <b>AS-3.5.4</b> <b>AS-3.5.5</b> <b>AS-3.5.6</b> <b>AS-3.5.7</b> <b>AS-3.5.8</b> AS-3.5.9 <b>AS-3.6.1</b> <b>AS-3.6.2</b> <b>AS-3.7.1</b> <b>BP-4.4.4</b> <b>BP-4.6.1</b> <b>BP-4.6.2</b> <b>IN-1.2.2</b> <b>IN-2.2.2</b>
CM-4 (1)	<b>CM-3.1.16</b> <b>AS-3.6.1</b>
CM-4 (2)	<b>CM-4.1.4</b> <b>AS-3.10.1</b>
CM-5	<b>CM-3.1.16</b> <b>CM-3.1.17</b> <b>AS-3.4.2</b> <b>AS-3.6.2</b> <b>AS-3.6.3</b> <b>AS-3.7.1</b> <b>AS-3.8.1</b> <b>AS-3.9.1</b> <b>AS-3.12.1</b> <b>BP-1.5.3</b>
CM-5 (1)	<b>CM-3.1.2</b> <b>AS-3.5.3</b>
CM-5 (2)	<b>CM-3.1.2</b> <b>AS-3.12.1</b>
CM-5 (4)	<b>CM-3.1.12</b> <b>AS-3.4.2</b>
CM-5 (5)	<b>CM-3.1.16</b> <b>CM-3.1.17</b> <b>AS-3.9.1</b>
CM-5 (6)	<b>CM-3.1.16</b> <b>CM-3.1.17</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
CM-6	<b>CM-2.1.3</b> AS-3.2.1 <b>AS-3.11.1</b> <b>AS-3.12.1</b>
CM-6 (1)	None
CM-6 (2)	<b>CM-4.1.4</b>
CM-7	<b>AC-3.1.7</b> <b>AC-3.1.9</b> <b>AC-3.2.1</b> AC-3.2.2 AC-3.2.3 <b>CM-2.1.3</b>
CM-7 (1)	<b>CM-4.1.1</b>
CM-7 (2)	<b>AS-4.2.1</b>
CM-7 (3)	<b>SM-1.5.1</b>
CM-8	<b>SM-1.5.1</b> <b>CM-2.1.1</b> CM-2.1.2
CM-8 (1)	<b>SM-1.5.1</b>
CM-8 (2)	None
CM-8 (3)	None
CM-8 (4)	SM-1.3.1
CM-8 (5)	<b>SM-1.5.1</b>
CM-8 (6)	None
CM-8 (7)	None
CM-8 (9)	<b>SM-1.5.1</b>
CM-9	<b>CM-1.1.1</b> <b>CM-3.1.1</b> <b>CM-4.1.3</b> <b>SD-1.1.2</b> <b>AS-3.1.1</b> <b>AS-3.3.1</b>
CM-9 (1)	None
CM-10	CM-3.1.19 CM-5.1.7 CM-5.1.8
CM-11	CM-3.1.19 CM-5.1.8
CM-11 (1)	CM-5.1.8
CM-11 (2)	CM-5.1.8

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
CP-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AS-1.1.1</b> AS-1.4.1 <b>AS-5.3.2</b> CP-3.1.1
CP-2	AC-6.5.1 <b>CP-1.2.1</b> <b>CP-1.2.2</b> <b>CP-1.3.1</b> CP-2.3.3 CP-3.1.1 CP-3.1.2 CP-3.1.3 CP-3.1.4 CP-3.1.5 CP-3.1.6 CP-3.1.7 CP-3.2.1 CP-3.2.3 <b>AS-5.1.1</b> AS-5.1.2 <b>AS-5.1.3</b> <b>AS-5.3.1</b> <b>AS-5.3.2</b> <b>AS-5.3.3</b>
CP-2 (1)	<b>AS-5.3.2</b>
CP-2 (2)	<b>CP-1.2.1</b> <b>CP-1.2.2</b>
CP-2 (3)	<b>CP-2.1.4</b>
CP-2 (4)	<b>CP-2.1.4</b>
CP-2 (5)	<b>CP-1.1.2</b> <b>AS-5.1.1</b>
CP-2 (6)	CP-2.1.3 <b>CP-2.1.4</b>
CP-2 (7)	None
CP-2 (8)	<b>CP-1.2.1</b> <b>AS-5.1.1</b>
CP-3	CP-2.3.1 CP-2.3.2
CP-3 (1)	CP-4.1.1 <b>AS-5.4.1</b>
CP-3 (2)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
CP-4	AC-6.5.1 CP-2.2.9 CP-2.3.4 CP-3.1.7 CP-4.1.1 CP-4.2.1 CP-4.2.2 <b>AS-5.4.1</b> <b>AS-5.4.2</b> <b>AS-5.4.3</b> <b>AS-5.4.4</b>
CP-4 (1)	None
CP-4 (2)	CP-2.1.3 <b>CP-2.1.4</b>
CP-4 (3)	None
CP-4 (4)	<b>AS-5.4.2</b>
CP-6	<b>CP-2.1.1</b> CP-2.1.2 CP-2.1.3 CP-3.2.1
CP-6 (1)	CP-2.1.3 CP-3.2.2 <b>AS-5.2.3</b>
CP-6 (2)	AS-5.1.2
CP-6 (3)	CP-3.2.1
CP-7	CP-3.2.1 CP-3.2.2 CP-2.1.3
CP-7 (1)	CP-2.1.3 CP-3.2.2 <b>AS-5.2.3</b>
CP-7 (2)	CP-3.2.1
CP-7 (3)	CP-3.2.2
CP-7 (4)	None
CP-7 (6)	<b>AS-5.4.2</b>
CP-8	CP-3.2.2
CP-8 (1)	CP-3.2.1
CP-8 (2)	CP-3.2.2
CP-8 (3)	CP-3.2.2
CP-8 (4)	None
CP-8 (5)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
CP-9	<b>CP-2.1.1</b> CP-2.1.2 <b>CP-2.1.4</b> <b>AS-5.2.1</b> <b>AS-5.2.2</b> <b>AS-5.2.3</b>
CP-9 (1)	<b>CP-2.1.4</b>
CP-9 (2)	None
CP-9 (3)	CP-2.4.5
CP-9 (5)	<b>CP-2.1.1</b>
CP-9 (6)	CP-3.2.1 CP-3.2.2 <b>AS-5.2.3</b>
CP-10	<b>CP-2.1.4</b>
CP-10 (2)	<b>CP-2.1.1</b>
CP-10 (4)	AS-5.1.2
CP-10 (6)	CP-2.1.3 <b>AS-5.2.3</b> <b>AS-5.3.3</b>
IA-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> AC-2.1.2 <b>AC-2.1.3</b> <b>AS-1.1.1</b> AS-1.4.1 <b>AS-2.2</b> <b>AS-2.3.1</b>
IA-2	<b>AC-2.1.1</b> AC-2.1.4 <b>AC-4.1.1</b> <b>AS-2.2</b> <b>AS-2.3.2</b>
IA-2 (1)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (2)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (3)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (4)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (5)	<b>AC-2.1.1</b> <b>AC-2.1.9</b>
IA-2 (6)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (7)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (8)	<b>AC-2.1.18</b>



## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
IA-2 (9)	<b>AC-2.1.18</b>
IA-2 (10)	None
IA-2 (11)	AC-2.1.4 <b>AS-2.2</b>
IA-2 (12)	None
IA-2 (13)	None
IA-3	<b>AC-1.1.3</b>
IA-3 (1)	<b>AC-1.1.3</b> AC-1.1.5
IA-3 (3)	None
IA-3 (4)	None
IA-4	<b>AC-2.1.1</b> AC-2.1.2 <b>AC-2.1.3</b> AS-2.3.3
IA-4 (1)	None
IA-4 (2)	None
IA-4 (3)	None
IA-4 (4)	None
IA-4 (5)	None
IA-4 (6)	None
IA-4 (7)	None
IA-5	<b>AC-2.1.5</b> <b>AC-2.1.6</b> <b>AC-2.1.8</b> <b>AC-2.1.9</b> <b>AC-2.1.10</b> <b>AC-2.1.11</b> <b>AC-2.1.12</b> <b>AC-2.1.13</b> <b>AC-2.1.15</b> <b>AC-2.1.16</b> <b>AC-3.1.7</b> AC-3.2.3 <b>AC-4.1.3</b> <b>AC-4.1.5</b> <b>AS-2.3.1</b>
IA-5 (1)	<b>AC-2.1.5</b> <b>AC-2.1.6</b> <b>AC-2.1.7</b> <b>AC-2.1.8</b> <b>AC-2.1.9</b> <b>AC-2.1.10</b>
IA-5 (2)	<b>AC-2.1.12</b> <b>AC-2.1.16</b>
IA-5 (3)	<b>AC-2.1.12</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
IA-5 (4)	None
IA-5 (5)	<b>AC-2.1.9</b> <b>AC-2.1.10</b> <b>AC-3.1.7</b>
IA-5 (6)	<b>AC-2.1.12</b> <b>AC-2.1.17</b>
IA-5 (7)	<b>AC-2.1.11</b>
IA-5 (8)	None
IA-5 (9)	<b>AC-2.1.12</b> <b>AC-3.2.3</b>
IA-5 (10)	<b>AC-3.2.3</b>
IA-5 (11)	AC-2.1.4
IA-5 (12)	AC-2.1.4
IA-5 (13)	None
IA-5 (14)	None
IA-5 (15)	None
IA-6	<b>AC-2.1.17</b>
IA-7	AC-4.3.3 <b>AC-2.1.16</b>
IA-8	<b>AC-2.1.1</b> AC-2.1.2
IA-8 (1)	None
IA-8 (2)	None
IA-8 (3)	None
IA-8 (4)	None
IA-8 (5)	None
IA-9	<b>AC-1.1.3</b> <b>AC-2.1.1</b>
IA-9 (1)	<b>SM-7.1.1</b>
IA-9 (2)	None
IA-10	AC-2.1.4
IR-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AC-5.1.1</b> AC-5.3.7 <b>AS-1.1.1</b> AS-1.4.1
IR-2	<b>AC-5.1.1</b>
IR-2 (1)	CP-4.1.1 <b>AS-5.4.1</b>
IR-3	<b>AC-5.1.1</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
IR-3 (2)	<b>AC-5.1.1</b> CP-3.1.1
IR-4	<b>AC-5.3.1</b> <b>AC-5.3.2</b> AC-5.3.6 AC-5.3.7
IR-4 (1)	None
IR-4 (2)	None
IR-4 (3)	None
IR-4 (4)	<b>AC-5.1.1</b>
IR-4 (5)	None
IR-4 (6)	None
IR-4 (7)	AC-5.3.6
IR-4 (8)	AC-5.3.6
IR-4 (9)	AC-5.3.7
IR-4 (10)	None
IR-5	AC-5.2.2 <b>AC-5.2.3</b> <b>AC-5.2.7</b>
IR-5 (1)	<b>AC-5.3.4</b>
IR-6	<b>AC-5.3.2</b> <b>AC-5.3.4</b> AC-5.3.6
IR-6 (1)	<b>AC-5.3.1</b>
IR-6 (2)	<b>AC-5.3.4</b>
IR-6 (3)	AC-5.3.6
IR-7	<b>AC-5.1.1</b>
IR-7 (2)	<b>AC-5.1.1</b>
IR-8	<b>AC-5.1.1</b>
IR-9	<b>AC-5.3.1</b> through AC-5.3.9
IR-9 (1)	<b>SM-1.1.1</b> <b>SM-4.1.1</b>
IR-9 (2)	<b>SM-1.1.1</b> <b>SM-4.1.1</b>
IR-9 (3)	<b>SM-1.1.1</b> <b>SM-4.1.1</b>
IR-9 (4)	<b>SM-1.1.1</b> <b>SM-4.1.1</b>
IR-10	AC-5.3.9

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
MA-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> CP-2.4.1 CP-2.4.6 <b>AS-1.1.1</b> AS-1.4.1
MA-2	AC-6.4.9 CP-2.4.2 CP-2.4.3 CP-2.4.4 CP-2.4.7 CP-2.4.8 CP-2.4.10 CP-2.4.11
MA-2 (2)	None
MA-4	<b>AC-4.1.3</b>
MA-4 (1)	<b>SM-7.1.1</b>
MA-4 (2)	SM-7.1.2
MA-4 (3)	None
MA-4 (4)	<b>SD-1.1.2</b>
MA-4 (5)	None
MA-4 (6)	None
MA-4 (7)	None
MA-6	CP-2.4.2 CP-2.4.5
MA-6 (1)	CP-2.4.2
MA-6 (2)	CP-2.4.10 CP-2.4.11
MA-6 (3)	None
MP-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AS-1.1.1</b> AS-1.4.1
MP-2	AC-4.2.1
MP-3	AC-4.2.2
MP-4	AC-4.2.4 AC-6.4.8 AC-6.4.9
MP-4 (2)	AC-6.4.8
MP-5	AC-4.2.3 AC-4.3.1 AC-6.3.7

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
MP-5 (3)	AC-4.2.3
MP-5 (4)	AC-4.3.1 AC-4.2.4
MP-6	AC-4.2.6
MP-6 (1)	AC-4.2.6
MP-6 (2)	AC-4.2.6
MP-6 (3)	AC-4.2.6
MP-6 (7)	None
MP-6 (8)	None
MP-7	<b>AC-1.1.7</b> SM-4.1.2
MP-7 (1)	<b>AC-1.1.7</b>
MP-7 (2)	None
MP-8	AC-4.2.1 AC-4.2.2 AC-4.2.4
MP-8 (1)	AC-4.2.6
MP-8 (2)	AC-4.2.4 <b>AC-4.2.5</b>
MP-8 (3)	AC-4.2.3 AC-4.2.6
MP-8 (4)	AC-4.2.3 AC-4.2.6
PE-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> AC-6.1.1 <b>AC-6.1.2</b> <b>AS-1.1.1</b> AS-1.4.1 AS-2.11.1 <b>DA-1.1.2</b>
PE-2	AC-6.1.9 <b>AC-6.3.1</b> <b>AC-6.3.2</b> <b>AC-6.3.3</b> AC-6.4.2 <b>AC-6.4.4</b> AS-2.11.1 <b>DA-1.1.2</b>
PE-2 (1)	<b>AC-6.3.1</b> <b>AC-6.3.2</b>
PE-2 (2)	AC-6.1.9
PE-2 (3)	AC-6.4.2

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
PE-3	<b>AC-6.1.2</b> AC-6.1.8 AC-6.1.9 AC-6.2.1 AC-6.2.2 AC-6.2.5 <b>AC-6.3.2</b> AC-6.3.7 AC-6.3.8 AC-6.4.2 <b>AC-6.4.3</b> AC-6.4.6 AC-6.4.7 AC-6.5.2 AS-2.11.1 <b>DA-1.1.1</b> <b>DA-1.1.2</b>
PE-3 (1)	<b>AC-6.1.2</b> <b>AC-6.4.3</b> <b>AC-6.4.4</b> AS-2.11.1
PE-3 (2)	AC-6.2.1 AC-6.3.7
PE-3 (3)	AC-6.2.1 AC-6.2.3 <b>AC-6.3.2</b> AC-6.3.4 AC-6.3.8
PE-3 (4)	None
PE-3 (5)	None
PE-3 (6)	None
PE-4	AC-6.4.8 AC-4.2.3
PE-5	<b>AC-6.3.2</b> AC-4.2.3
PE-5 (1)	AC-4.2.1 <b>AC-6.4.3</b>
PE-5 (2)	None
PE-5 (3)	None
PE-6	AC-6.1.7 AC-6.2.3 AC-6.3.4 AC-6.3.5 AC-6.3.8 <b>AC-6.3.3</b> <b>AC-6.4.4</b> AC-6.4.5 AC-6.5.3 AS-2.11.1 <b>DA-1.1.2</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
PE-6 (1)	AC-6.3.4
PE-6 (2)	AC-6.1.7
PE-6 (3)	AC-6.3.8
PE-6 (4)	<b>AC-6.4.3</b> <b>AC-6.4.4</b> AC-6.4.5
PE-8	AC-6.1.9 AC-6.3.5 AC-6.4.2
PE-8 (1)	None
PE-9	CP-2.2.2 CP-2.2.3 CP-2.2.6 <b>AC-6.4.3</b>
PE-9 (1)	AC-6.4.10 CP-2.2.3
PE-9 (2)	CP-2.2.6
PE-10	CP-2.2.2 CP-2.2.8
PE-11	AC-6.4.10 CP-2.2.2 CP-2.2.3 CP-2.2.5
PE-11 (1)	None
PE-11 (2)	None
PE-12	AC-6.2.4 CP-2.2.2 CP-2.2.7
PE-12 (1)	AC-6.2.4
PE-13	CP-2.2.1 CP-2.2.2
PE-13 (1)	CP-2.2.1
PE-13 (2)	CP-2.2.1
PE-13 (3)	CP-2.2.1
PE-13 (4)	CP-2.2.9
PE-14	CP-2.2.3 CP-2.2.6
PE-14 (1)	CP-2.2.6
PE-14 (2)	CP-2.2.6
PE-15	CP-2.2.2 CP-2.2.4
PE-15 (1)	CP-2.2.1 CP-2.2.4
PE-16	AC-6.3.7

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
PE-17	CP-2.2.2 CP-2.2.3 CP-3.2.2 CP-3.2.3
PE-18	CP-2.2.2 CP-2.2.4
PE-18 (1)	CP-2.2.2
PL-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AS-1.1.1</b> AS-1.4.1 AS-1.5.4
PL-2	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 SM-1.3.1 <b>SM-1.4.1</b> <b>SM-1.4.2</b> <b>SM-3.1.1</b> <b>CM-5.1.2</b> <b>CM-5.1.4</b> <b>AS-1.1.1</b> <b>AS-2.1.1</b>
PL-2 (3)	<b>SM-1.1.1</b> SM-1.2.1 SM-1.2.2 SM-1.3.1 <b>SM-1.4.1</b> <b>SM-1.4.2</b> <b>AS-1.1.1</b>
PL-4	SM-4.1.2 CP-2.2.10
PL-4 (1)	<b>SM-4.1.1</b> SM-4.1.2
PL-7	<b>SM-3.1.1</b>
PS-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>SM-4.1.1</b> <b>AS-1.1.1</b>
PS-2	SM-4.2.1 SM-4.2.2
PS-3	SM-4.2.1 SM-4.2.2
PS-3 (1)	SM-4.2.1 SM-4.2.2
PS-3 (2)	SM-4.2.1 SM-4.2.2



## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
PS-3 (3)	SM-4.2.1 SM-4.2.2
PS-4	<b>SM-4.2.6</b>
PS-4 (1)	<b>SM-4.2.6</b>
PS-4 (2)	None
PS-5	<b>SM-4.2.6</b>
PS-6	SM-4.1.2 SM-4.2.3
PS-6 (2)	SM-4.2.1 SM-4.2.3
PS-6 (3)	<b>SM-4.2.6</b>
PS-7	<b>SM-7.1.1</b> SM-7.1.2 AC-6.1.6 <b>AS-1.7.1</b> AS-1.7.2
PS-8	<b>SM-4.2.5</b> <b>AC-5.3.3</b>
RA-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-2.1.1</b> <b>SM-3.1.1</b> <b>AS-1.1.1</b> <b>AS-1.2.1</b> AS-1.4.1
RA-2	<b>SM-2.1.2</b> <b>CP-1.1.1</b> <b>CP-1.1.2</b>
RA-3	<b>SM-2.1.3</b> <b>SM-2.1.4</b> <b>SM-2.1.5</b> AC-6.1.1 AC-6.1.3 AC-6.5.4 <b>AS-1.2.1</b>
RA-5	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>
RA-5 (1)	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>
RA-5 (2)	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>
RA-5 (3)	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
RA-5 (4)	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>
RA-5 (5)	None
RA-5 (6)	None
RA-5 (8)	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>
RA-5 (10)	<b>SM-5.1.2</b> <b>CM-5.1.1</b> <b>AS-3.13.1</b>
RA-6	<b>SM-2.1.1</b> <b>AS-1.2.1</b>
SA-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>SM-7.1.1</b> <b>AS-1.1.1</b> AS-1.4.1
SA-2	SM-1.2.1
SA-3	<b>AS-3.3.1</b>
SA-4	SM-7.1.2
SA-4 (1)	SM-7.1.2
SA-4 (2)	SM-7.1.2
SA-4 (3)	SM-7.1.2
SA-4 (5)	SM-7.1.2
SA-4 (6)	SM-7.1.2
SA-4 (7)	SM-7.1.2
SA-4 (8)	SM-7.1.2
SA-4 (9)	SM-7.1.2
SA-4 (10)	SM-7.1.2
SA-5	<b>SM-1.1.1</b> <b>CM-2.1.1</b> <b>AS-1.1.1</b>
SA-8	CM-1.1
SA-9	<b>SM-7.1.1</b>
SA-9 (1)	<b>SM-7.1.1</b>
SA-9 (2)	<b>SM-7.1.1</b>
SA-9 (3)	<b>SM-7.1.1</b>
SA-9 (4)	<b>SM-7.1.1</b>
SA-9 (5)	<b>SM-7.1.1</b> SM-7.1.2

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SA-10	<b>CM-3.1.14</b> <b>CM-3.1.15</b> <b>CM-3.1.17</b> CM-3.1.18
SA-10 (1)	<b>CM-3.1.14</b>
SA-10 (2)	None
SA-10 (3)	None
SA-10 (4)	<b>CM-1.1.1</b>
SA-10 (5)	<b>CM-1.1.1</b>
SA-10 (6)	<b>CM-1.1.1</b>
SA-11	<b>CM-3.1.5</b> <b>CM-3.1.6</b> <b>CM-3.1.7</b> <b>CM-3.1.8</b> <b>CM-3.1.9</b> CM-3.1.10 <b>CM-3.1.11</b> <b>CM-3.1.12</b>
SA-11 (1)	<b>CM-1.1.1</b>
SA-11 (2)	<b>CM-1.1.1</b>
SA-11 (3)	<b>CM-1.1.1</b>
SA-11 (4)	<b>CM-1.1.1</b>
SA-11 (5)	<b>CM-1.1.1</b>
SA-11 (6)	<b>CM-1.1.1</b>
SA-11 (7)	<b>CM-1.1.1</b>
SA-11 (8)	<b>CM-1.1.1</b>
SA-12	<b>SM-1.1.1</b> CM-1.1 <b>AS-1.1.1</b>
SA-12 (1)	<b>CM-1.1.1</b> SM-7.1.2
SA-12 (2)	<b>SM-1.1.1</b> SM-7.1.2 <b>CM-1.1.1</b>
SA-12 (5)	None
SA-12 (7)	<b>SM-1.1.1</b> <b>CM-1.1.1</b>
SA-12 (8)	None
SA-12 (9)	None
SA-12 (10)	None
SA-12 (11)	None
SA-12 (12)	<b>SM-7.1.1</b> SM-7.1.2
SA-12 (13)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SA-12 (14)	<b>SM-1.1.1</b> <b>CM-1.1.1</b> <b>AS-1.1.1</b>
SA-12 (15)	<b>SM-6.1.1</b>
SA-13	<b>SM-1.1.1</b> <b>AS-1.1.1</b>
SA-14	<b>AS-1.1.1</b>
SA-15	<b>CM-3.1.16</b>
SA-15 (1)	<b>SM-7.1.1</b>
SA-15 (2)	<b>SM-7.1.1</b> SM-7.1.2
SA-15 (3)	<b>SM-7.1.1</b> SM-7.1.2
SA-15 (4)	<b>SM-7.1.1</b> SM-7.1.2
SA-15 (5)	<b>SM-7.1.1</b> SM-7.1.2 <b>CM-1.1.1</b>
SA-15 (6)	<b>SM-7.1.1</b> SM-7.1.2
SA-15 (7)	None
SA-15 (8)	None
SA-15 (9)	<b>SM-7.1.1</b> SM-7.1.2
SA-15 (10)	<b>SM-7.1.1</b> SM-7.1.2
SA-15 (11)	<b>SM-7.1.1</b> SM-7.1.2
SA-16	<b>SM-4.3.2</b>
SA-17	<b>SM-1.1.1</b>
SA-17 (1)	<b>SM-7.1.1</b> SM-7.1.2
SA-17 (2)	<b>SM-7.1.1</b> SM-7.1.2
SA-17 (3)	None
SA-17 (4)	None
SA-17 (5)	None
SA-17 (6)	None
SA-17 (7)	<b>SM-7.1.1</b> SM-7.1.2
SA-18	<b>AC-5.3.8</b>
SA-18 (1)	None
SA-18 (2)	None
SA-21	SM-4.2.1 SM-4.2.2 <b>AC-3.1.1</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SA-21 (1)	<b>SM-7.1.1</b>
SC-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AS-1.1.1</b> AS-1.4.1
SC-2	<b>AC-4.1.8</b>
SC-2 (1)	<b>AC-4.1.8</b>
SC-3	<b>AC-4.1.9</b>
SC-3 (1)	None
SC-3 (2)	None
SC-3 (3)	None
SC-3 (4)	None
SC-3 (5)	None
SC-5	<b>AC-5.1.1</b>
SC-5 (1)	None
SC-5 (2)	None
SC-5 (3)	None
SC-6	SM-1.2.1 <b>CP-1.2.2</b>
SC-7	<b>AC-1.1.2</b> <b>AC-3.2.1</b> CP-2.4.5 CP-2.4.6 <b>AS-2.1.1</b> <b>AS-2.5.1</b>
SC-7 (3)	<b>AC-1.1.1</b>
SC-7 (4)	<b>AC-1.1.1</b>
SC-7 (5)	None
SC-7 (7)	None
SC-7 (8)	None
SC-7 (9)	None
SC-7 (10)	None
SC-7 (11)	None
SC-7 (12)	None
SC-7 (13)	<b>AC-4.1.9</b>
SC-7 (14)	<b>AC-6.1.2</b> AC-6.1.8
SC-7 (15)	None
SC-7 (16)	None
SC-7 (17)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SC-7 (18)	None
SC-7 (19)	<b>AC-1.1.1</b> <b>AC-1.1.2</b>
SC-7 (20)	None
SC-7 (21)	None
SC-7 (22)	None
SC-7 (23)	None
SC-8	AC-4.3.1
SC-8 (1)	AC-4.3.1 AC-4.3.2
SC-8 (2)	AC-4.3.1 AC-4.3.2
SC-8 (3)	AC-4.3.1 AC-4.3.2
SC-8 (4)	None
SC-10	AC-1.2.2
SC-11	AC-4.1.10
SC-11 (1)	None
SC-12	AC-4.3.1 AC-4.3.4
SC-12 (1)	AC-4.3.1 AC-4.3.4
SC-12 (2)	AC-4.3.1 AC-4.3.4
SC-12 (3)	AC-4.3.1 AC-4.3.4
SC-13	AC-4.3.1 <b>AS-2.5.1</b> <b>AS-2.7.1</b>
SC-15	AC-3.2.4
SC-15 (1)	None
SC-15 (3)	None
SC-15 (4)	None
SC-16	<b>AC-4.2.5</b>
SC-16 (1)	None
SC-17	<b>AC-2.1.15</b> <b>AS-2.5.1</b>
SC-18	AC-4.1.6
SC-18 (1)	None
SC-18 (2)	None
SC-18 (3)	None
SC-18 (4)	None
SC-18 (5)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SC-19	CM-5.1.6
SC-20	AC 2.1.18
SC-20 (2)	AC-2.1.18
SC-21	<b>AC-2.1.18</b>
SC-22	<b>AC-2.1.18</b>
SC-23	<b>AC-1.2.1</b> AC-1.2.2 AC-2.1.14 <b>AC-2.1.18</b>
SC-23 (1)	AC-1.2.2
SC-23 (3)	<b>AC-2.1.18</b>
SC-23 (5)	<b>AC-2.1.16</b>
SC-28	AC-4.3.1
SC-28 (1)	AC-4.3.1
SC-28 (2)	AC-4.3.1 CP-2.1.2
SC-32	<b>CM-3.1.16</b> <b>AS-3.6.1</b> <b>AS-3.6.2</b> <b>DA-1.1.2</b>
SC-36	<b>CP-2.1.1</b> CP-2.1.3
SC-36 (1)	None
SC-37	<b>AC-1.1.2</b>
SC-37 (1)	None
SC-38	<b>CM-1.1.1</b> <b>AS-3.3.1</b>
SC-40	<b>AC-1.1.2</b> AC-1.1.6 <b>AC-1.1.7</b>
SC-41	<b>BP-1.3.1</b>
SC-43	AC-4.1.6 CM-3.1.19 CM-5.1.6 CM-5.1.7
SI-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>CM-5.1.2</b> <b>CM-5.1.4</b> <b>AS-1.1.1</b> AS-1.4.1 <b>BP-1.1.1</b>
SI-2	<b>AC-1.1.7</b> <b>CM-5.1.3</b>

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SI-2 (1)	None
SI-2 (2)	None
SI-2 (3)	None
SI-2 (5)	None
SI-2 (6)	None
SI-3	<b>AC-1.1.7</b> AC-3.2.5
SI-3 (1)	None
SI-3 (2)	<b>AC-1.1.7</b>
SI-3 (4)	None
SI-3 (6)	None
SI-3 (7)	None
SI-3 (8)	None
SI-3 (9)	None
SI-3 (10)	None
SI-4	AC-3.2.5 <b>AC-5.2.1</b> <b>AC-5.3.8</b> AC-5.3.9
SI-4 (1)	None
SI-4 (2)	<b>DA-1.2.2</b>
SI-4 (3)	None
SI-4 (4)	None
SI-4 (5)	<b>AC-5.1.1</b>
SI-4 (7)	None
SI-4 (9)	None
SI-4 (10)	None
SI-4 (11)	None
SI-4 (12)	None
SI-4 (13)	None
SI-4 (14)	AC-1.1.6
SI-4 (15)	None
SI-4 (16)	None
SI-4 (17)	None
SI-4 (18)	None
SI-4 (19)	None
SI-4 (20)	None
SI-4 (21)	None
SI-4 (22)	None
SI-4 (23)	None



## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SI-4 (24)	None
SI-5	<b>AC-1.1.7</b> AC-5.3.5 <b>CM-5.1.2</b> <b>CM-5.1.3</b>
SI-5 (1)	None
SI-6	<b>CM-4.1.4</b>
SI-6 (2)	None
SI-6 (3)	<b>CM-4.1.4</b>
SI-7	AC-3.2.5 AC-4.3.1 <b>AC-5.3.8</b> <b>CM-4.1.1</b> <b>CM-4.1.2</b>
SI-7 (1)	<b>CM-4.1.4</b>
SI-7 (2)	None
SI-7 (3)	None
SI-7 (5)	<b>CM-4.1.4</b>
SI-7 (6)	AC-4.3.1
SI-7 (7)	<b>AC-5.1.1</b>
SI-7 (8)	AC-5.2.2
SI-7 (9)	None
SI-7 (10)	None
SI-7 (11)	None
SI-7 (12)	None
SI-7 (13)	None
SI-7 (14)	None
SI-7 (15)	AC-4.3.1
SI-7 (16)	<b>AS-2.4.3</b>
SI-8	<b>CM-5.1.4</b> <b>AC-1.1.2</b>
SI-8 (1)	None
SI-8 (2)	<b>CM-5.1.4</b>
SI-8 (3)	<b>CM-5.1.4</b>

## NIST SP 800-53 to FISCAM Overview Mapping

<b>NIST 800-53 Control Number</b>	<b>FISCAM Control Technique</b>
SI-10	AC-3.2.5 <b>BP-1.2.1</b> <b>BP-1.3.1</b> <b>BP-1.4.1</b> <b>BP-1.5.1</b> <b>BP-1.5.2</b> <b>BP-1.5.3</b> <b>BP-1.6.1</b> <b>BP-1.7.1</b> <b>BP-1.8.1</b> <b>BP-2.1.1</b> <b>BP-2.3.1</b> <b>BP-2.3.2</b> <b>BP-4.1.1</b> <b>BP-4.1.2</b> <b>BP-4.1.3</b> <b>BP-4.3.1</b> <b>BP-4.3.2</b> <b>IN-1.2.3</b>
SI-10 (1)	<b>BP-1.5.2</b>
SI-10 (2)	<b>BP-1.7.1, IN-2.4.1</b>
SI-10 (3)	None
SI-10 (4)	<b>IN-2.1.1</b>
SI-10 (5)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SI-11	<b>BP-1.7.1</b> <b>BP-1.8.1</b> <b>BP-2.2.1</b> <b>BP-2.2.2</b> <b>BP-2.2.3</b> <b>BP-2.3.1</b> <b>BP-2.4.1</b> BP-2.4.2 <b>BP-2.4.3</b> <b>BP-2.4.4</b> BP-3.1.1 <b>BP-3.2.1</b> <b>BP-3.2.3</b> <b>BP-3.3.1</b> <b>BP-3.3.2</b> <b>BP-3.3.3</b> BP-3.5.1 BP-3.5.2 <b>BP-4.3.2</b> <b>BP-4.4.4</b> <b>IN-1.1.1</b> <b>IN-1.2.1</b> <b>IN-1.2.3</b> <b>IN-2.2.1</b> <b>IN-2.2.3</b> <b>IN-2.4.1</b> <b>IN-2.5.1</b> <b>IN-2.5.2</b> <b>IN-2.5.3</b>
SI-12	AC-4.2.1 AC-4.2.2 AC-4.2.3 AC-4.2.4 <b>AC-4.2.5</b> AC-4.2.6 <b>AC-5.2.7</b> AC-6.4.8 BP-3.1.1 <b>BP-3.2.1</b> BP-3.2.2 <b>BP-3.3.1</b> <b>BP-3.3.2</b> <b>BP-3.3.3</b> <b>BP-3.4.1</b> BP-3.5.1 BP-3.5.2
SI-13	<b>CP-1.2.1</b> <b>CP-1.2.2</b> CP-2.4.6
SI-13 (1)	CP-3.1.1
SI-13 (2)	None

## NIST SP 800-53 to FISCAM Overview Mapping

NIST 800-53 Control Number	FISCAM Control Technique
SI-13 (3)	CP-3.1.1
SI-13 (4)	CP-2.4.5
SI-13 (5)	CP-3.1.1
SI-15	BP-3.1.1 <b>BP-3.2.1</b> BP-3.2.2 <b>BP-3.2.3</b> <b>BP-3.3.1</b> <b>BP-3.3.2</b> <b>BP-3.3.3</b> <b>BP-3.4.1</b>
SI-17	<b>CP-1.3.1</b> <b>CP-2.1.4</b> CP-2.3.3 CP-2.3.4
PM-1	<b>SM-1.1.1</b> <b>SM-1.1.2</b> SM-1.2.1 <b>SM-3.1.1</b> <b>AS-1.1.1</b> AS-1.4.1
PM-2	SM-1.2.2
PM-4	<b>SM-6.1.1</b> SM-6.1.2 <b>SM-6.1.3</b>
PM-5	<b>SM-1.5.1</b>
PM-6	CP-2.4.9
PM-8	AC-6.1.1
PM-9	<b>SM-1.1.1</b> <b>SM-5.1.1</b> AC-6.1.1
PM-10	<b>AC-1.1.1</b> <b>AC-1.2.1</b> <b>AC-3.1.1</b> <b>AC-3.2.1</b> <b>AC-4.1.1</b> AC-4.2.1 AC-4.3.1 <b>AS-2.1.1</b> <b>AS-2.2</b> <b>AS-2.3.1</b> <b>AS-2.4.1</b> <b>AS-2.5.1</b> <b>AS-2.6.1</b> <b>AS-2.7.1</b>
PM-11	<b>SM-1.4.1</b> <b>AS-1.1.1</b>

NIST SP 800-53 to FISCAM Overview Mapping	
NIST 800-53 Control Number	FISCAM Control Technique
PM-14	SM-4.3.1 <b>SM-4.3.2</b> <b>AC-1.1.2</b> <b>AS-1.1.1</b>
PM-16	AC-5.3.6 AC-6.1.4

### Detailed Mapping of FISCAM Control Techniques to NIST SP 800-53 Controls



FISCAM to NIST  
Mapping.pdf



NIST to FISCAM  
Mapping.pdf