BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 65-201

17 SEPTEMBER 2020

Financial Management

ENTERPRISE RISK MANAGEMENT AND MANAGERS' INTERNAL CONTROL PROGRAM PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms for downloading or ordering are available on the e-Publishing website at **www.e-publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/FMFA

Certified by: SAF/FM
(Mr. John Roth)

Supersedes: AFI 65-201, 9 February 2016

Pages: 37

This instruction implements Air Force Policy Directive 65-2, *Enterprise Risk Management and Managers' Internal Control Program*. It provides a structure to establish, evaluate, and report on Air Force Risk Management and internal controls in all functional areas including Special Access Programs based on recognized leading practices and in compliance with the Office of Management and Budget (OMB) Circular Number (No.) A-123 *Management's Responsibility for Enterprise Risk Management and Internal Control* requirements. This instruction applies to all civilian employees and uniformed members of the Regular Air Force, Air Force Reserve, and Air National Guard. This Air Force instruction may be supplemented at any level, but all supplements that directly implement this instruction must be routed to "SAF/FMFA" for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the Air Force Form 847, *Recommendation for Change of Publication*; route Air Force Forms 847 from the field through the appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Instruction 33-322, *Records Management and Information Governance Program, and disposed of in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information*

Management System." Changes are underlined to identify revisions; do not actually underline these parts of the statement in the draft publication.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Enterprise Risk Management requirements have been added throughout this instruction to comply with OMB Circular No. A-123 and Department of Defense Instruction 5010.40 *Enterprise Risk Management and Managers' Internal Control Program*. Accordingly, a new chapter was added on Risk Management. A new chapter was also added to provide guidance for internal control over operations activities. A Governance paragraph was added in **Chapter 1** to identify OMB Circular No. A-123 governing bodies and associated responsibilities. References have been made throughout this instruction to the A-123 Playbook for more detailed internal control and risk management guidelines that need to be followed. The A-123 Playbook will be updated annually by SAF/FMF to align with the Department of Defense and Air Force priorities, as well as applicable federal, departmental, and branch financial management requirements. The A-123 Playbook builds upon previous activities, progress, and accomplishments, and defines current internal control initiatives.

Chapter 1—GOALS AND RESPONSIBILITIES **5**

1.1. Introduction. 5

1.2. Objectives. 5

1.3. Internal Control Standards. 5

1.4. Governance. 5

1.5. Roles and Responsibilities. 6

Chapter 2—RISK MANAGEMENT **8**

2.1. Overview. 8

2.2. Risk Management Practices. 8

2.3. Information Technology Risk Management Framework. 8

Chapter 3—INTERNAL CONTROL OVER REPORTING **9**

3.1. Overview. 9

3.2. Reasonable Assurance. 9

3.3. Internal Control Standards. 9

3.4. Assessment. 10

3.5. Materiality. 11

3.6. Material Weaknesses. 11

Chapter 4—INTERNAL CONTROL OVER FINANCIAL SYSTEMS 13

4.1. Overview. 13

4.2. Internal Control Standards. 13

4.3. Assessment. 14

4.4. Reliability. 15

Chapter 5—INTERNAL CONTROL OVER OPERATIONS 16

5.1. Overview. 16

5.2. Internal Control Standards. 16

5.3. Assessment. 16

5.4. Material Weaknesses. 16

Chapter 6—INTERNAL CONTROL PROCEDURES 17

6.1. Risk Management and Internal Control Program. 17

6.2. Segmentation. 17

6.3. Management Control Plan. 18

6.4. Risk Assessment. 18

6.5. Internal Control Assessment. 19

6.6. Corrective Action Plan: 21

Chapter 7—STATEMENT OF ASSURANCE REPORTING 23

7.1. General. 23

7.2. Air Force Statement of Assurance: 23

7.3. Supporting Statements of Assurance: 23

7.4. Concept of Reasonable Assurance: 24

7.5. Classification of Control Deficiencies. 24

7.6. Material Weakness Quarterly Reporting: 26

7.7. Material Weakness Tracking System: 26

Chapter 8—SPECIAL CONSIDERATIONS 28

8.1. Special Access Programs. 28

8.2. Freedom of Information Act (FOIA) Implications: 28

8.3. Host Tenant Relationships: 28

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 30

Attachment 2—REPORTING CATEGORIES 35

Chapter 1

GOALS AND RESPONSIBILITIES

1.1. Introduction. To meet the requirement of Title 31 United States Code (USC) Section 3512, Executive agency accounting and other financial management reports and plans. Also referred to as "Federal Managers' Financial Integrity Act of 1982, the Department of the Air Force must establish, evaluate and report on internal controls, and submit an annual Statement of Assurance to the Department of Defense.

1.2. Objectives. An Enterprise Risk Management approach and the Managers' Internal Control Program establish the framework for the Air Force to assess the design, implementation and effectiveness of internal controls and provide reasonable assurance that internal controls meet three objectives:

1.2.1. Effectiveness and efficiency of operations

1.2.2. Reliability of financial reporting

1.2.3. Compliance with applicable laws and regulations

1.3. Internal Control Standards. Federal Managers have the fundamental responsibility to establish and maintain internal controls in accordance with OMB Circular No. A-123, and the Government Accountability Office (GAO)-14-704-G, Standards for Internal Control in the Federal Government (also referred to as the "GAO Green Book").". OMB Circular No. A-123 outlines five components which provide the basis for evaluating the system of internal controls at the entity level. Each is explained in greater detail in the A-123 Playbook. The five components are:

1.3.1. Control Environment

1.3.2. Risk Assessment

1.3.3. Control Activities

1.3.4. Information and Communications

1.3.5. Monitoring

1.4. Governance. AFPD 65-2 establishes a governance structure to effectively implement, direct and oversee implementation of OMB Circular No. A-123 and all the provisions of a robust process of risk management and internal control.

1.4.1. Management must use the Enterprise Risk Management framework to identify new or emerging risks, and/or changes in existing risks. **(T-0).**

1.4.2. Management must evaluate the effectiveness of internal controls annually using the Government Accountability Office Green Book and OMB Circular No. A-123. **(T-0).**

1.4.3. Refer to the A-123 Playbook for the internal control organizational structure and governing bodies' roles and responsibilities. This A-123 Playbook serves as a standard reference for users involved in reporting internal control activities within Air Force. This includes the requirements required of the Federal Managers' Financial Integrity Act of 1982, the OMB Circular No. A-123, and other applicable laws, regulations, and guidance.

1.4.4. Key governance bodies include:

1.4.4.1. A Senior Management Council is required to assess and monitor deficiencies in internal control. The Senior Management Council is responsible for overseeing the timely implementation of corrective actions related operational significant deficiencies and material weaknesses. The Senior Management Council will identify, analyze, and respond to significant changes that could impact the internal control program. The Senior Management Council is chaired by the Air Force Deputy Chief Management Officer (DCMO) with the Air Force Assistant DCMO serving as the alternate chair, and members of senior leadership from the reporting elements and other major reporting organizations.

1.4.4.2. A Risk Management Council will be used, as required, to oversee the establishment of the Air Force's risk profile, continuously assess risks and develop an appropriate risk response. The Risk Management Council is chaired by the Air Force Deputy Chief Management Officer (DCMO) with the Air Force Assistant DCMO serving as the alternate chair, and members of senior leadership from the reporting elements and other major reporting organizations. An effective Risk Management Council will include senior officials for program operations and mission-support functions to help ensure those risks are identified which have the most significant impact on the mission outcomes of the Department of the Air Force. Responsibilities include defining clear objectives to build a risk strategy, enabling the identification of risks, establishing a risk profile, and defining risk tolerances. The Risk Management Council is involved in the identification, analysis, and response to risks related to achieving the defined objectives. The Risk Management Council will consider the potential for fraud when identifying, analyzing, and responding to risks. Additionally, the Risk Management Council is involved with the identification, analysis, and response to significant changes that could impact the internal control system.

1.4.4.3. The Senior Assessment Team is responsible for overseeing the timely implementation of corrective actions related to financial reporting, financial systems and compliance significant deficiencies and material weaknesses. The Senior Assessment Team is comprised of senior level executives and provides oversight over assessing and documenting the effectiveness of internal controls and risk management. It is responsible for ensuring; 1) objectives are clearly communicated, 2) assessment is carried out in an effective and timely manner, 3) adequate funding and resources are made available, 4) staff/contractors to perform assessments are identified, 5) scope of the assessment, and 6) the assessment design and methodology are determined.

1.5. Roles and Responsibilities. The Risk Management and Internal Control Program roles are inherently governmental. Only civilian employees and/or military members of the Air Force, to include direct-hire foreign national employees, are authorized to serve in those roles. Contractors or indirect-hire foreign national employees are not authorized to serve in the Risk Management and Internal Control Program roles. However, contractors may assist with most administrative tasks related to the preparation of the Statement of Assurance. Refer to the A-123 Playbook for roles and responsibilities related to internal control and risk management.

1.5.1. Assessable Unit Managers must:

1.5.1.1. Apply controls to all administrative, operational, and programmatic functions as well as accounting and financial management; **(T-0).**

1.5.1.2. Ensure internal control costs do not exceed the expected benefits; **(T-0).**

1.5.1.3. Use the annual Statement of Assurance to report; **(T-0).**

1.5.1.4. Compliance with the Federal Managers Financial Integrity Act;

1.5.1.5. Operational, financial reporting, and financial systems compliance with applicable laws and regulations; and

1.5.1.6. Internal control material weaknesses and the corrective action plan to mitigate material weaknesses.

1.5.1.7. Actively identify and escalate potential risks that could impede or impair the delivery of the strategic objectives specific to their functional organization.

1.5.1.8. As required, act as a risk owner when appropriate based on their unique subject matter expertise

Chapter 2

RISK MANAGEMENT

2.1. Overview. OMB Circular No. A-123 defines management's responsibilities for Enterprise Risk Management (ERM) and includes requirements for identifying and managing risks. Key requirements include the development of an initial and comprehensive Risk Profile in line with their annual strategic review process. In addition, OMB Circular No. A-123 requires the development of an ERM maturity model and supporting implementation plan inclusive of full integration with existing internal control program(s). Together, these requirements help enable agencies to consider the full spectrum of risks on a holistic basis to better inform decision making to maximize value to the taxpayer and enable the delivery of strategic objectives. A fully functioning OMB Circular No. A-123 program will provide the Air Force with a more proactive, top-down and risk-based approach that can enable a reduction in external auditor findings, flag risks as they emerge, and manage a prioritized portfolio of risks on an on-going basis. The Air Force A-123 Playbook and Statement of Assurance Handbook are updated annually to reflect the Air Force's approach to risk management in line with approved governance, statement of assurance reporting deadlines, and formalized policies and procedures for managing enterprise risks through life.

2.2. Risk Management Practices.

2.2.1. Risk Management Practices are forward-looking to identify existing and potential risks as proactively as possible based on the approved Enterprise Risk Taxonomy, with an emphasis on financial reporting, financial systems, and operational business processes.

2.2.2. Risk Management Practices are designed to assist Air Force leadership with making better decisions to manage both existing and emerging risks, as well as identify opportunities to improve the efficiency and effectiveness of operations.

2.2.3. Enterprise risks may be identified as:

2.2.3.1. Specific to a wing, base, major command, or reporting element.

2.2.3.2. Enterprise-wide (i.e. applicable at an Air Force level).

2.2.3.3. Contributing to facilitating significant deficiencies in the Department of Defense. **(T-0).**

2.2.3.4. All risks will be considered based on agreed likelihood and impact scales, with the identified Air Force Risk Officer ultimately being responsible for the Air Force enterprise risk profile and Statement of Assurance risk assessment inputs. In addition to likelihood/impact scoring, risks will be considered based on level of alignment to strategic objectives as well as the potential to adversely impact mission delivery.

2.2.3.5. Fraud risk is managed within the Department of the Air Force in accordance with the Fraud Reduction and Data Analytics Act and OMB Circular No. A-123.

2.3. Information Technology Risk Management Framework. Refer to AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT).

Chapter 3

INTERNAL CONTROL OVER REPORTING

3.1. Overview. Internal control over reporting is embedded in business processes to assist in providing reasonable assurance regarding the reliability of reporting. It begins with the initiation of a transaction and ends with its reporting in the financial statements. Therefore, internal controls involve activities at every step of the end-to-end business process, including the control activities over transaction initiation, maintenance of records and or assets, the recording of transactions, and final reporting. In addition, it includes the prevention or detection of unauthorized acquisition, and use/or disposition of assets in relation to the transaction. Refer to the A-123 Playbook for additional information regarding Internal Controls over Reporting objectives.

3.2. Reasonable Assurance. OMB Circular No. A-123 Appendix A requires the following assertions for reasonable assurance over financial reporting.

3.2.1. All reported transactions occurred during the reporting period and all assets and liabilities exist as of the reporting date (existence and occurrence);

3.2.2. All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (completeness);

3.2.3. All assets are legally owned by the Department of the Air Force and all liabilities are legal obligations of the Department of the Air Force (rights and obligations);

3.2.4. All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation);

3.2.5. The financial report is presented in the proper form and any required disclosures are present (presentation and disclosure);

3.2.6. The transactions are in compliance with applicable laws and regulations;

3.2.7. All assets have been safeguarded against fraud and abuse; and

3.2.8. Documentation for internal control, all transactions, and other significant events is readily available for examination.

3.3. Internal Control Standards. Management is responsible for developing, documenting and maintaining internal control activities over financial reporting that comply with the following OMB and the GAO Green Book: **(T-0).**

3.3.1. Control Environment: Understanding management's attitude, awareness, and actions, clearly defined authority and responsibility, appropriate delegation of authority and responsibility, integrity and ethical standards, commitment to competence, hierarchy for reporting, proper support for human capital hiring, training, advancing and disciplining to ensure individuals are held accountable for their internal control responsibilities.

3.3.2. Risk Assessment: Identifying internal and external risks including the potential for fraud, taking into account previous audit findings, internal management reviews, noncompliance with laws, regulations and policies; then analyzing risk for potential effect and impact. Some significant events can affect risk. These include complexity or magnitude

of programs or new operations, extent of manual processes, related party transactions, decentralized versus centralized accounting, accounting estimates, new programs, personnel, technology, or amended laws, regulations or accounting standards.

3.3.3. Control Activities: The policies, procedures, and mechanisms in place that ensure management's directives are carried out, such as proper segregation of duties, physical control over assets, proper authorization, appropriate documentation and access to documentation, analytical review and analysis, and safeguarding information.

3.3.4. Information and Communication: Includes obtaining an understanding of the financial systems, communicating the duties and responsibilities to personnel for proper handling of internal and external information, planning for disaster recovery, and determining the type and sufficiency of reports produced.

3.3.5. Monitoring: Management shall conduct periodic reviews to determine effectiveness of internal controls through self-assessment and determine remediation plans for any identified deficiency, direct testing or evaluations from the Inspector General, auditors, or other assessment organizations. **(T-1).** The assessment will include obtaining an understanding of the major types of activities the Department of the Air Force uses to monitor internal control over reporting and how those activities are used to initiate corrective actions.

3.4. Assessment. OMB Circular No. A-123 Appendix A prescribes a process for management to assess internal control over reporting. The process:

3.4.1. Evaluates internal controls at the entity level, which encompasses the five components of internal controls described in section 3.3.

3.4.2. Evaluates internal control at the process, transaction, or application levels. Management's knowledge of daily operations, significant accounts or groups of accounts, major classes of transactions, understanding the financial reporting process, understanding control design, ability to identify controls not adequately designed, test controls and assess compliance to support management's assertions. Obtains knowledge of the organization's key processes through performance of process risk assessments of financial assertions, providing reasonable assurance of completeness, rights and obligations, valuation, existence and occurrence, presentation and disclosure, as well as compliance with laws and regulations; while safeguarding assets from fraud, waste, and abuse and identifying existing key controls intended to mitigate identified risk.

3.4.2.1. The degree to which all AUMs understand and adhere to the GAO *Standards for Internal Control in the Federal Government* and the OMB Circular A-123.

3.4.3. Assesses and tests the design and operation of internal control over reporting. The assessment should determine whether internal controls are appropriately designed and operating effectively and identify if a material weakness exists in the design or operation.

3.4.4. Assesses internal control over reporting using a variety of information sources, including those specific to internal control reviews or as a by-product of other reviews, such as Inspector General, Government Accountability Office, and Air Force Audit Agency audit reports. **(T-1).** The assessment of internal control over reporting should be coordinated with other activities to avoid duplication of efforts with similar activities.

3.4.5. Documents the entire assessment process for deficiencies and development of corrective action plans. Documentation can be electronic or hard copy and shall be readily available for review. Documentation shall be maintained for weaknesses that are downgraded from a significant deficiency to a control deficiency in order to support management decisions. **(T-0).**

3.4.6. Issues a Statement of Assurance of internal control over reporting as a subset of the annual Statement of Assurance. The statement must take one of the following forms: unmodified, modified, or statement of no assurance. **(T-0).**

3.5. Materiality. Risk assessments under internal control over reporting must contain a materiality assessment that may include risk that affect financial reporting with specific focus on those business events that significantly increase or decrease financial statement balances. Refer to the A-123 Playbook for the annual materiality calculation which is determined using guidance from the Federal Audit Manual. Other qualitative factors such as transaction volume, program visibility, or command directed focus areas may also be considered in determining materiality. **(T-0).**

3.6. Material Weaknesses. An internal control over reporting material weakness is a significant deficiency in which the secretary of the Air Force determines significant enough to impact internal or external decision-making and reports outside of the Air Force as a material weakness. The material weaknesses deficiency criteria are defined within the A-123 Playbook. Corrective action milestones for Internal Controls Over Reporting material weakness are reported as part of the corrective action plans.

3.6.1. All Air Force deficiency owners will monitor the progress of corrective action plans for material weaknesses impacting their organization or function. **(T-0).** Corrective action of internal control over reporting material weaknesses:

3.6.1.1. Require prompt resolution of corrective actions. **(T-0).**

3.6.1.2. Require the appointment of senior accountable officials who will report to the Senior Assessment Team. **(T-0).**

3.6.2. Rating officials must assure that performance appraisals of senior accountable officials reflect effectiveness in resolving or implementing corrective action for the identified material weakness in accordance with the OMB Circular No. A-123, chapter V, Correcting Internal Control Deficiencies; and the GAO Green Book. **(T-0).**

3.6.3. Air Force deficiency owners will maintain accurate records on the status of the identified material weaknesses through the entire process of resolution and corrective action. **(T-0).**

3.6.4. Air Force deficiency owners will assure that the corrective action plans are consistent with laws, regulations, and administrative policy. Significant deficiencies and material weaknesses requires validation to ensure the controls are effective. This determination shall be made in writing and include supporting documentation available for review by the Senior Assessment Team. A determination that a material weakness has been corrected should be made only when sufficient corrective actions have been taken and the desired results are achieved consistent with **Paragraph 6.6** Corrective action plans shall include validation

milestones which evaluates and certifies the design and effectiveness of the corrective action. (T-0)

Chapter 4

INTERNAL CONTROL OVER FINANCIAL SYSTEMS

4.1. Overview. Air Force financial systems managers who develop, deploy or sustain information systems will effectively develop and maintain internal controls over financial systems. This chapter prescribes Air Force instruction for achieving compliance with the 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plans (referred to as the Federal Financial Management Improvement Act of 1996). The FFMIA requires that each Federal Government agency establish and maintain financial management systems that substantially comply with the following three requirements: federal financial management system requirements, applicable federal accounting standards, and the USSGL at the transaction level. OMB Circular No. A-123 Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996, provides goals and compliance indicators that must be satisfied in order for financial management systems to comply with FFMIA. In accordance with the FFMIA and OMB Circular No. A-123 Appendix D, the Air Force strategy for compliance is integrated with related efforts to achieve auditability and maintain effective internal control over reporting. Documentation that supports these related requirements also support FFMIA compliance and may be used to avoid duplication of efforts. **(T-0).**

4.2. Internal Control Standards. Management shall ensure the effectiveness of security controls over information resources that support Air Force operations and assets. **(T-1).** The two broad groups of information system controls are application controls that cover the processing of financial data within the application software, and general controls that apply to all mainframe, minicomputer and network systems (core financial systems). These controls are interrelated; both are needed to ensure complete and accurate information processing.

4.2.1. Management shall ensure the controls are adequate and are proportionate with the risk. **(T-1).**

4.2.2. Management shall prepare a report on the effectiveness of the internal control over financial systems. **(T-1).**

4.2.3. Management shall disclose material weaknesses in the statement of assurance and must include specific plans and schedules for corrective actions. **(T-0).** Each material weakness corrective action plan will follow procedures as described in **paragraph 6.6** and shall include a validation milestone which evaluates and certifies the design and effectiveness of the corrective action.

4.2.4. The internal control over financial systems statement of assurance is based on the results of assessments completed in accordance with the following authorities:

4.2.4.1. 31 U.S.C. 3512 ensures that federal financial management systems provide accurate, reliable, and timely financial management information to the government's managers.

4.2.4.2. Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, (44 U.S.C. 3553) provides several modifications that modernize federal security practices to address evolving security concerns.

4.2.4.3. OMB Circular No. A-123 and in particular Appendix D of this Circular re-examined existing financial systems policy to ensure they meet the purposes of the Federal Financial Management Improvement Act (FFMIA) of 1996.

4.2.4.4. OMB Circular No. A-130, Management of Federal Information Resources establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy.

4.2.4.5. OMB Circular No. A-136, Financial Reporting Requirements establishes reporting guidance for Executive Branch entities required to submit audited financial statements.

4.2.4.6. Department of Defense (DoD) 7000.14-R, Volume 1, Financial Management Regulation (FMR): General Financial Management Information, Systems and Requirements, **Chapter 3**.

4.2.4.7. Department of Defense Instruction 8510.01, Risk Management Framework for DoD Information Technology.

4.2.4.8. American Institute of Certified Public Accountants, Statement on Standards for Attestation Engagements (SSAE) No. 18, Attestation Standards: Clarification and Recodification.

4.2.4.9. Treasury Financial Manual (TFM), Volume 1, Part 6, Chapter 9500, Revised Federal Financial Management System Requirements for Fiscal Reporting.

4.2.4.10. National Institute of Standards and Technology, Standard Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

4.3. Assessment. Management should implement risk and evidence-based assessments that leverage existing audit tests, evaluations, and reviews that auditors and others already perform. Key considerations when determining compliance with FFMIA requirements include, but are not limited to, the following:

4.3.1. Management must have controls over information which is not directly transferred from the accounting system to the financial report, but requires intervening calculation, summarizations, etc. **(T-1).**

4.3.2. Data transfers to core financial systems must be traceable to the transaction source and posted to the core financial system in accordance with the Federal Accounting Standards Advisory Board (is a United States federal advisory committee whose mission is to improve federal financial reporting through issuing federal financial accounting standards), to include the United States Standard General Ledger (USSGL) which provides a uniform chart of accounts and technical guidance for standardizing federal agency accounting. **(T-1).**

4.3.3. Controls must be in place to ensure completeness, accuracy, authorization, and validity of all transactions during application processing. **(T-1).**

4.3.4. Data centers and client-server operation controls will include backup and recovery procedures, contingency and disaster recovery plans. **(T-1).**

4.3.5. Access security controls must be in place to prevent un-authorized internal and external access, such as identification and authentication, security configuration, physical access and system penetration. **(T-1).**

4.3.6. Management must consider system software internal controls including control over the acquisition, implementation, and maintenance of all system software. **(T-1).**

4.3.7. Controls shall be established at an application's interface to verify inputs and outputs. **(T-1).**

4.4. Reliability. Substantial compliance with internal control over financial systems is achieved when the Department of the Air Force's financial management systems routinely provide reliable and timely financial information for managing day-to-day operations as well as produce reliable financial statements, maintain effective internal control, and comply with legal and regulatory requirements.

Chapter 5

INTERNAL CONTROL OVER OPERATIONS

5.1. Overview. Internal control over operations provides assurance on the effectiveness and efficiency of operations for each entity as it pertains to the overall program, operational, and the administrative controls relevant to all mission-essential functions. The assurance shall be based on the results of management's assessment conducted according to the requirements of OMB Circular No. A-123 and the GAO Green Book. Refer to the A-123 Playbook for additional information regarding Internal Controls over Operations objectives.

5.2. Internal Control Standards. Management shall ensure the effectiveness of controls over operations. **(T-1).**

5.2.1. Management shall ensure the controls are adequate and are proportionate with the risk. **(T-1).**

5.2.2. Management shall disclose material weaknesses in the Statement of Assurance and must include specific plans and schedules for corrective actions. **(T-0).** Each material weakness corrective action plan will follow procedures as described in **paragraph 6.6** and shall include validation milestone(s) which evaluate(s) and certifies the design and effectiveness of the corrective action.

5.2.3. Air Force Instruction 90-2001, Mission Sustainment, outlines the purpose and responsibilities of the Headquarters Air Force, major command, and installation Mission Sustainment Working Groups.

5.2.4. The internal control over operations Statement of Assurance is based on the results of assessments completed in accordance with; the Federal Financial Management Improvement Act of 1996, Public Law 104-208, Title VIII (31 U.S.C. 3512 note), OMB Circular No. A-123, DoD 7000.14-R, Vol 1, and the GAO Green Book.

5.3. Assessment. The Internal Control over Operations assessment process is similar to the internal control over reporting Assessment process described in **paragraphs 3.4.1** through **3.4.5** of this document.

5.4. Material Weaknesses. Air Force Instruction 38-401, Continuous Process Improvement, outlines the responsibilities of the Enterprise Process Improvement Council from a Continuous Process Improvement perspective. The A-123 Playbook Governance section describes the role the Enterprise Process Improvement Council plays regarding approving, tracking, and reporting internal control over operations "significant deficiencies" and "material weaknesses".

Chapter 6

INTERNAL CONTROL PROCEDURES

6.1. Risk Management and Internal Control Program. The Air Force will implement Risk Management and Internal Control Program at all levels. An integrated program requires a top-down approach to provide leadership direction on strategic objectives and risks to determine the scope of internal control assessments. It also requires a bottoms-up approach to collect and report on testing results and effectiveness in order to assess enterprise risk exposure and strategic objectives. This will be accomplished through formal guidance and policies driven from OUSD as well as supplementary guidance specific to the Air Force through the A-123 Playbook. The "SAF/FM" A-123 team will be the primary team responsible for coordinating with stakeholders at all levels of the organization to provide subject matter expertise, formal/informal training, and address open questions to support implementation. **(T-1).** Leadership includes, as part of their basic management philosophy, a culture to sustain organizational support for internal controls and internal control processes to improve effectiveness and accountability for results. Periodic assessments should be integrated as part of management's continuous monitoring of internal control. To the greatest extent possible, Risk Management and Internal Control Program should be consolidated with daily operating and management practices and utilize existing evaluative processes. Assessable unit managers will implement the Managers' Internal Control Program as follows:

6.1.1. Segment the organization into assessable units. Divide each primary and subordinate reporting organization into entities capable of being evaluated by internal control assessment procedures as outlined in **paragraph 6.5** **(T-1).**

6.1.2. Develop a Management Control Plan as defined in **paragraph 6.3** **(T-1).**

6.1.3. Perform a risk assessment to identify potential hazards that prevents the assessable unit from achieving its objectives, document findings and implement the internal controls necessary to mitigate the risks as defined in **paragraph 6.4** **(T-1).**

6.1.4. Conduct and document internal control assessments, as described in **paragraph 6.5** **(T-1).**

6.1.5. Develop and implement corrective action plans for identified deficiencies and weaknesses as outlined in **paragraph 6.6** **(T-1).**

6.2. Segmentation.

6.2.1. All major commands, the Air Force Operational Test and Evaluation Center, United States Air Force Academy, Air Force District of Washington, Air National Guard, and Army Air Force Exchange Service are designated primary reporting elements of the Air Force Managers' Internal Control Program. Resource Directorate, Office of Administrative Assistant to the Secretary of the Air Force (SAF/AAR), serves as the primary reporting element for all Secretariat and Air Staff offices. The heads of these organizations are the Air Force's highest-level assessable unit managers who direct the Managers' Internal Control Program within their organizations and are required to submit a consolidated Statement of Assurance to the Component Managers' Internal Control Program Manager at SAF/FMFA. **(T-0).**

6.2.2. Primary reporting elements should be segmented along organizational, programmatic, or functional lines into assessable units so that all subcomponents or organizations under the direct authority, supervision, and/or responsibility of the Department of the Air Force are identified as a separate and distinct assessable unit or are included as a part of another assessable unit. The sum of the assessable unit encompasses the entire organization. No Air Force activity or program is exempt from the requirements of the Managers' Internal Control Program. This includes all personnel assigned to Air Force organizations and reporting organizations for which the Air Force serves as the executive agent.

6.2.3. Primary reporting elements may determine how far the segmentation should progress in order to achieve adequate oversight of internal control responsibilities. Designate assessable units of appropriate nature and size that a single manager may be held responsible for the assessment of internal controls. To the extent practical, standardize assessable units and associated internal controls for the operation of common functions and activities throughout organizations. assessable units are mandated to meet the following criteria: **(T-0).**

6.2.3.1. Have clear limits or boundaries and be identifiable to a specific responsible manager;

6.2.3.2. Be large enough to allow observations that provide reasonable assurance that internal controls are in place and adequate, but not so large that any material weakness goes un-detected. The Assessable Unit Administrator should have a span of control to be able to actively participate in the review process.

6.2.3.3. For activities or functions that are contracted out, Air Force managers performing related functions that are inherently governmental in nature (for example, property accountability, contract administration, and quality assurance) must form the assessable unit over that activity or function. **(T-1).**

6.3. Management Control Plan. Responsibilities of the MICP follow the chain of command.

6.3.1. Primary reporting elements shall establish and maintain a comprehensive Management Control Plan detailing the primary reporting element's assessable units and the processes and procedures for conducting the Managers' Internal Control Program. **(T-1).** An assessable unit inventory is maintained in a Management Control Plan which should be updated at least annually. **(T-1).**

6.3.2. The Management Control Plan includes, at a minimum: number of assessable units, title of each assessable unit, responsible assessable unit manager, date of last Management Control Program review, responsible Assessable Unit Administrator, status of assessable unit manager training, material weaknesses and significant deficiencies, if reported, and corrective action plans, if applicable. **(T-0).**

6.4. Risk Assessment.

6.4.1. Prior to assessing risk, management must establish a clear mission and objectives for the assessable unit. **(T-1).**

6.4.2. A risk assessment determines where a potential hazard exists that might prevent the organization from achieving its objectives. The risk assessment should be consistent with the Risk Management policy outlined within OMB Circular No. A-123 and updated as policies,

procedures and missions change within the assessable unit. The following questions assist with identifying risks:

6.4.2.1. What could go wrong in the process?

6.4.2.2. What processes require the most judgment?

6.4.2.3. What processes are the most complex?

6.4.2.4. What has to go right for mission success?

6.4.2.5. How could we fail to accomplish our objectives?

6.4.2.6. How do we know whether we are achieving our objectives?

6.4.2.7. Where are our vulnerable areas?

6.4.3. Management should identify and document risks that are internal and external to the organization as a part of standard operating procedures. Specific analysis methods can vary by organization due to varying mission requirements and difficulty assigning qualitative and quantitative risk levels. Management should consider the significance of the risk (low, medium, high), likelihood and impact of occurrence, and what actions should be taken. Management should also consider the following when assessing risk: previous reports and findings; e.g., auditor identified, results of internal management reviews, non-compliance with laws, regulations, policies and procedures within the organization.

6.4.4. Management should consider mechanisms for assessing special risks associated with changing environment and mission conditions. Existing risk management programs and tools should be leveraged where possible. Procedures and policies outlined in Air Force Instruction AFI 90-802, Risk Management, may be used as a basis for Managers' Internal Control Program risk assessments; however, safety programs alone do not address all potential risks an assessable unit may face in accomplishing its mission and safeguarding its assets. Risk assessments, as a part of safety programs, contribute to, but do not likely fully satisfy the assessable unit manager's responsibility to assess risks under the Managers' Internal Control Program.

6.4.5. Refer to **Chapter 2** Risk Management and the A-123 Playbook for additional guidance pertaining to Risk Management.

6.5. Internal Control Assessment.

6.5.1. Assessable unit managers, or delegated Assessable Unit Administrators, are responsible for continuously monitoring their internal controls.

6.5.2. All internal control assessment stakeholders should review their respective process cycle memorandums to gain an understanding of the Air Force standard for a particular business process (i.e. Civilian Pay, Military Equipment, etc.). Process cycle memorandums are discussed in more detail in the A-123 Playbook.

6.5.3. Internal control assessments are performed by or at the direction of Assessable Unit Administrators to determine whether internal controls exist, are correctly implemented, and to ensure that internal control systems are working effectively to mitigate risks. Internal control assessments are of two broad types: 1) a specific detailed examination of internal controls in a prescribed review format especially designed for that purpose, (see **paragraph**

6.5.5) or 2) using a variety of assessment processes that provide adequate information regarding the effectiveness of control techniques (see **paragraph 6.5.4**).

6.5.4. The following internal control over reporting assessment phases should be used to develop a viable internal control testing approach and provide a framework for the internal control assessment procedures outlined in this chapter. Specific guidance associated with each phase can be found in the A-123 Playbook.

6.5.4.1. Planning Phase

6.5.4.1.1. Entity Level Control Assessment and Risk Assessments

6.5.4.1.2. Information Technology Materiality

6.5.4.1.3. Fraud Risk

6.5.4.1.4. Significant Line Items

6.5.4.1.5. Identification of Primary Cycles for Significant Line Items and assessable units

6.5.4.1.6. Statement of Assurance Execution Handbook

6.5.4.1.7. Governance Structure

6.5.4.2. Documentation Phase

6.5.4.2.1. Management Review Controls

6.5.4.2.2. Process Cycle Memos

6.5.4.2.3. Walkthroughs

6.5.4.2.4. Service Providers

6.5.4.2.5. Document Retention Guidelines

6.5.4.3. Testing Phase

6.5.4.3.1. Test Plan

6.5.4.3.2. Test of Design

6.5.4.3.3. Test of Effectiveness

6.5.4.4. Evaluation Phase

6.5.4.4.1. Internal Control Deficiencies

6.5.4.4.2. Deficiency Type

6.5.4.4.3. Summary of Aggregated Deficiencies

6.5.4.5. Reporting phase

6.5.4.5.1. Reporting Schedule

6.5.4.5.2. Corrective Action Plan

6.5.5. Assessable Unit Administrators must:

6.5.5.1. Develop and communicate a written description of the organization's goals and corresponding internal controls. These descriptions may already exist in current regulations, standard operating procedures, and other similar documentation. **(T-1).** If the observed controls differ from the assessable unit's written description, the Assessable Unit Administrator will update the description of the controls. **(T-1).**

6.5.5.2. Evaluate their internal controls so that excessive controls can be eliminated, and weak controls can be improved. **(T-1).**

6.5.5.3. Ensure internal control assessments are documented and the documentation is maintained as a part of the Assessable Unit Administrator's Internal Control Program and in compliance with Air Force Records Information Management System. **(T-1).**

6.5.6. In order to streamline the process of reviewing internal control systems, DoDI 5010.40, encourages managers to rely on existing internal control reviews. Managers shall not duplicate existing reviews that have included a specific assessment of internal controls and are properly documented. **(T-1).** Managers are encouraged to utilize the following sources of information for existing internal control assessments:

6.5.6.1. Management and oversight reviews

6.5.6.2. Computer security reviews

6.5.6.3. Air Force Audit Agency, Department of Defense Inspector General and Government Accountability Office audits, inspections, or investigations, annual assessments performed in accordance with other statutory requirements such as the Federal Information Security Management Act, Government Performance and Results Act, and Improper Payments Elimination and Recovery Act.

6.5.6.4. System compliance reviews

6.5.6.5. Program evaluations

6.5.6.6. Self-inspection program, Staff Assist Visits

6.5.6.7. Unit Compliance Inspections

6.5.6.8. Quality Assurance reviews

6.5.7. If an existing assessment of controls is not available, then an appropriate internal control review is performed for the assessable unit. Locally developed review formats are used and shall be completed with consideration of the Internal Control Standards (**paragraph 1.3**).

6.6. Corrective Action Plan:

6.6.1. The deficiency owner must prepare, implement, and validate a corrective action plan for all internal control material weaknesses as they are identified. Refer to the Air Force Deficiency Acceptance and Corrective Action Plan Process Guide for guidance on accepting and documenting the remediation process associated with external and self-identified deficiencies. **(T-1).** The correction of internal control weaknesses is an integral part of management accountability and is considered a priority.

6.6.2. The recommendations for corrective action correlate with the risk. In some cases, management should strengthen the existing controls, and in others, management should

include new controls. Assessable unit managers must always consider the materiality of the weakness and the cost implications of actions to correct it when determining a corrective action plan. **(T-1).**

6.6.3. A corrective action plan identifies specific actions and completion dates for correcting the material weakness. The plan lists the tasks, called milestones, together with interim target dates for accomplishment. Milestones may be revised as required. The final milestone is one of verifying that the corrective actions achieved the desired results.

6.6.4. For internal control deficiencies that are not included as material weaknesses in the Statement of Assurance, corrective actions are developed and tracked internally at the appropriate level.

6.6.5. The performance appraisal of the responsible senior management official for correction of material weaknesses reported in the Secretary's Statement of Assurance evaluates the effective and timely resolution of the material weakness in accordance with DoDI 5010.40.

Chapter 7

STATEMENT OF ASSURANCE REPORTING

7.1. General. The reports relating to the Managers' Internal Control Program have been assigned Report Control Symbol DD- Comp AR 1618. The Office of the Undersecretary of Defense, Comptroller issues reporting guidelines and formats for all required reports. SAF/FM will issue appropriate call letters to primary reporting elements transmitting the prescribed guidance and current reporting formats.

7.2. Air Force Statement of Assurance:

7.2.1. SAF/FM will prepare the Air Force Statement of Assurance according to instructions received from the Office of the Undersecretary of Defense, Comptroller. The statement is submitted to satisfy the requirement outlined in the Federal Managers' Financial Integrity Act. The statement provides reasonable assurance of the effectiveness of Air Force internal controls, from the Secretary of the Air Force. A single cover memorandum states the senior management assessment as to whether or not there is reasonable assurance that the Air Force's internal controls are in place and operating effectively in three distinct processes:

7.2.1.1. Operational and administrative controls assessment relevant to all mission-essential functions throughout the Air Force;

7.2.1.2. Financial reporting assessment relevant to the Air Force General Fund and the Air Force Working Capital Fund functions assessed under the oversight of the Senior Assessment Team; and,

7.2.1.3. Financial Systems Assessment relevant to the integrated financial management system's conformance with Federal requirements.

7.2.2. The Statement of Assurance provides an assessment of the five components of internal control across the enterprise. These five components are explained in the GAO Green Book.

7.2.3. In cases where the Statement of Assurance provides a "Reasonable Assurance" or "No Assurance," the area or areas in question are specified and related to material weaknesses being reported.

7.2.4. The body of the statement provides a description of how the Managers' Internal Control Program was implemented during the year, improvements and innovations to the program, overview of training, disclosure of material weaknesses, descriptions of the plans and schedules for correcting those weaknesses and provides the status of corrective actions on prior year weaknesses.

7.3. Supporting Statements of Assurance:

7.3.1. Each primary reporting element must submit a supporting operational and administrative control Statement of Assurance that provides an overall level of assurance. **(T-1).** These supporting statements formulate the collective basis for the Secretary's Statement of Assurance. Refer to the A-123 Playbook and the Statement of Assurance Handbook for additional guidance.

7.3.2. The Statement of Assurance completed at the subordinate level may disclose weaknesses of varying degrees of significance to the primary reporting element as a whole. Management shall collect, analyze and document those crosscutting weaknesses or items common to several units and other significant deficiencies and consider whether they are appropriate for inclusion in the Statement of Assurance to the next higher-level official. **(T-1).** Reference DoDM 5200.01 volume 3, DoD Information Security Program: Protection of Classified Information, to ensure documents containing potential weaknesses and deficiencies are properly marked and safeguarded if necessary.

7.4. Concept of Reasonable Assurance:

7.4.1. In the context of the Federal Managers' Financial Integrity Act, "reasonable assurance" refers to a satisfactory level of management confidence that internal controls are adequate and operating as intended. Reasonable assurance recognizes that acceptable levels of risk exist due to outside factors which cannot be avoided or the cost of management's ability to achieve absolute control would exceed the benefits derived. The determination of reasonable assurance is a subjective management judgment. The subjectivity of this judgment can be reduced significantly by considering the following:

7.4.1.1. The degree to which all assessable unit managers understand and adhere to the GAO Green Book and the OMB Circular No. A-123.

7.4.1.2. The degree to which Assessable Unit Administrators are held formally accountable for the effectiveness of their internal controls and are evaluated on their performance in this regard.

7.4.1.3. The timeliness, adequacy, and results of internal control evaluations, including the correction of any internal control weaknesses detected.

7.4.1.4. Assessments from other sources (for example, audits, inspections, and investigations); media coverage; and direct management reviews or assessments by senior officials.

7.4.1.5. Supporting Statement of Assurance from subordinate Assessable Unit Administrators.

7.5. Classification of Control Deficiencies.

7.5.1. Deficiencies in internal controls must be reported if they are deemed to be material to the assessable unit. **(T-1).**

7.5.2. Organizations must report deficiencies that are either material enough to warrant the attention of more senior management or require the participation of more senior management to resolve. **(T-1).** As part of the aggregation process, senior management may delete less significant control deficiencies and may add new items which apply at more senior organizational levels. Thus, what may be a material weakness at one level may not be material at the next higher level. If the decision is made to exclude a material weakness during the reporting process, this decision must be documented and retained as a part of the assessable nit Management Control Program for review. **(T-1).** This process culminates with the primary reporting element reporting their most significant internal control problems in their supporting Statement of Assurance.

7.5.3. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to satisfactorily accomplish their assigned functions or inhibits the prevention or detection of misstatements on a timely basis. Control deficiencies are internal to the assessable unit and listed in the Management Control Program of the reporting assessable unit.

7.5.4. A significant deficiency is a deficiency or combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A significant deficiency specifically related to financial reporting is a control deficiency, or combination of control deficiencies, that adversely affects the organization's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles. The criteria for a significant deficiency mean that there is more than a remote likelihood that a misstatement of the financial statements that is more than inconsequential will not be prevented or detected. Significant deficiencies are internal to the assessable unit and listed in the Management Control Program of the reporting assessable unit.

7.5.5. To be considered material, a weakness must meet the following two conditions:

7.5.5.1. It must involve a weakness in internal controls, such as the controls are not in place, are not being used or are inadequate. Resource deficiencies in themselves are not internal control weaknesses.

7.5.5.2. It must warrant the attention of the next level of command, either because that next level must act or because they must be aware of the problem. This requires management's judgment, particularly in determining whether the next level of command must be aware of a weakness. The fact that a weakness can be corrected at one level does not exclude it from being reported to the next level; demonstrating the ability to effectively identify internal control weaknesses is one of the primary reasons for reporting a material weakness.

7.5.6. A material weakness is a significant deficiency where the Secretary of the Air Force determines to be significant enough to report externally as a material weakness.

7.5.6.1. A material weakness in internal control over operations might include conditions that:

7.5.6.1.1. Impact the operating effectiveness of Entity- Level Controls;

7.5.6.1.2. Impair fulfillment of essential operations or mission;

7.5.6.1.3. Deprive the public of needed services; or;

7.5.6.1.4. Significantly weaken established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest.

7.5.6.2. A material weakness in internal control over reporting is a significant deficiency in which the secretary of the Air Force determines significant enough to impact internal or external decision-making and reports outside of the Air Force as a material weakness.

7.5.6.3. A material weakness in internal control over external financial reporting is a deficiency, or a combination of deficiencies, in internal control, such that there is a

reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

7.5.6.4. A material weakness in internal control over compliance is a condition where management lacks a process that reasonably ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving Air Force's objectives.

7.5.6.5. A material weakness can be identified by other organizations, such as the Office of the Secretary of Defense functional offices, Government Accountability Office, Department of Defense Inspector General, or Air Force Audit Agency. assessable unit managers, with assistance from the Assessable Unit Administrators, should consider these recommendations and work toward a consensus on material weakness reporting with these offices.

7.6. Material Weakness Quarterly Reporting:

7.6.1. All primary reporting elements must provide a quarterly update on the status of corrective actions related to open material weaknesses to the SAF/FMFA. **(T-1).** The first and second quarterly updates are due on the tenth business day after the end of the quarter. The submission of the primary reporting element's Statement of Assurance serves as the third quarter update and the coordination and review of the Air Force Statement of Assurance serves as the fourth quarter update.

7.6.2. Identify and report all material weaknesses according to standard Department of Defense Internal Control reporting categories. See **Attachment 2** for the list of reporting categories.

7.7. Material Weakness Tracking System:

7.7.1. SAF/FMFA will maintain a summary of all material weaknesses and self-identified deficiencies by utilizing the Office of the Deputy Chief Financial Officer (ODCFO) database. primary reporting elements must maintain a subordinate system to track their own material weaknesses. **(T-1).** Information in the tracking system must include the Internal Control Reporting Category, narrative description of the problem, corrective action milestone chart and the name of the responsible official and point of contact for corrective action progress.

7.7.2. A material weakness may be reported as closed only after corrective actions are verified as effective. This verification may be completed by specific management reviews, follow-on audits, metric tracking, or other independent validation. There must be sufficient time, at least one quarter, between implementation of the final corrective action and verification of the corrective actions to demonstrate internal controls are working properly in normal operations. The verification shall be documented, and the documentation maintained as a part of the Air Force's weakness tracking system and shall be maintained in accordance with Air Force Manual 33-363. **(T-0).**

7.7.3. When possible, the audit follow-up process as required in AFI 65-301, Financial Management Internal Audit Services may be used to track the planned corrective actions for each internal control weakness stemming from audit reports. Corrective action plans must be consistent with corrective action status reports in the audit follow-up process.

7.7.4. All material weaknesses are documented and tracked throughout the fiscal year on the Office of the Deputy Chief Financial Officer Appendix D: Material weaknesses and Significant Deficiencies. Associated risks are documented in the Risk Template tracked throughout the fiscal year on Appendix F: Risk Assessment. This information is part of the Air Force Statement of Assurance submission and is described in more detail in the Air Force Statement of Assurance Handbook.

Chapter 8

SPECIAL CONSIDERATIONS

8.1. Special Access Programs. Air Force Special Access Programs are established and maintained when it is necessary to protect the most sensitive capabilities, information, technologies, and operations or when otherwise mandated by statute. The Air Force must establish controls, infrastructure and processes to manage, execute and protect the Special Access Programs. Key roles and responsibilities for establishing a Special Access Program are identified in Air Force Instruction 16-701 Management, Administration and Oversight of Special Access Programs. **(T-1).**

8.1.1. Primary reporting elements have overall responsibility for their Special Access Programs assessable units and will report an unclassified level of assurance for the Special Access Programs internal controls in their Statement of Assurance. **(T-1).**

8.1.2. Special Access Programs are required to align their Managers' Internal Control Program efforts to comply with the guidance outlined in this instruction, where possible.

8.1.3. "SAF/FMBIB" is responsible for policy, oversight, program review/site visits, and training of all special program activities for Managers' Internal Control Program purposes.

8.1.4. Each Special Access Program's assessable unit manager will provide a Statement of Assurance through their chain of command up to their primary reporting element with a copy to SAF/FMBIB. **(T-1).**

8.2. Freedom of Information Act (FOIA) Implications:

8.2.1. The Department of the Air Force statement of assurance may be made available, upon request, to the public, except in the case of any statement containing restricted information. The Federal Managers' Financial Integrity Act specifies that information in the following categories be deleted from the Statement before it is made available to the public:

8.2.1.1. Information specifically prohibited from disclosure by any provision of law.

8.2.1.2. Information specifically required by Executive Order to be kept secret in the interest of national defense or the conduct of foreign affairs.

8.2.1.3. All other requests for information are to be handled in accordance with procedures for release of information established by Department of Defense Manual 5400.07_AFMAN 33-302, Freedom of information Act Program.

8.3. Host Tenant Relationships:

8.3.1. Tenant units on other major command bases must perform internal control evaluations at the direction of the tenant unit's parent command. **(T-1).**

8.3.2. The Program Administrator will make recommendations to the commander where functions overlap or where functional Offices of Primary Responsibility disagree over who has responsibility for a certain action. **(T-1).**

JOHN P. ROTH
Assistant Secretary of the Air Force
(Financial Management)

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Title 31 United States Code (USC) Section 1352, *Limitation on use of appropriated funds to influence certain federal contracting financial transactions (also referred to as the Federal Managers Integrity Act)*

Public Law 114-186, *Fraud Reduction and Data Analytics Act of 2015*

Public Law 97-255, *Federal Managers' Financial Integrity Act*, 31 U.S.C. 3512

31 USC § 3512, *Executive agency accounting and other financial management reports and plans, Federal Financial Management Improvement Act of 1996 (FFMIA),* Title VIII

Pub. Law 113-283, *Federal Information Security Modernization Act of 2014 (FISMA),* (44 U.S.C. 3553)

Public Law 111-352, *Government Performance and Results Act*, January 4, 2011

Public Law 111–204, *Improper Payments Elimination and Recovery Act*, July 22, 2010

Treasury Financial Management, Volume 1, Part 6, Chapter 9500, *Revised Federal Financial Management System Requirements for Fiscal Reporting*, current edition

United States Standard General Ledger

OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, 15 July 2016

OMB Circular No. A-123 Appendix D, *Compliance with the Federal Financial Management Improvement Act of 1996*, 20 September 2013

OMB Circular No. A-130, *Management of Federal Information Resources,* 28 November 2000

OMB Circular No. A-136, *Financial Reporting Requirements*, 28 June 2019

OMB Circular No. A-123 Appendix A, *Management of Reporting and Data Integrity Risk,* 6 June 2018

GAO-14-704G, *Standards for Internal Control in the Federal Government*, 10 September 2014

DoD 7000.14-R, Vol 1, Financial Management Regulation (FMR): *General Financial Management Information, Systems and Requirements*, January 2020

DODM 5200.01, *DoD Information Security Program: Protection of Classified Information,* 24 February 2012

DoDI 5010.40, *Managers' Internal Control Program Procedures* 30 May 2013

DoDI 5400.07_Air Force Manual 33-302, *Freedom of Information Act Program,* 27 April 2018

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* 12 March 2014

DoD Directive (DoDD) 5000.01, *The Defense Acquisition System,* 12 May 2003

OUSD ATL Memorandum, *Guidance on the Assessment of Acquisition Functions under OMB Circular No. A-123*, 6 April 2009

Air Force Policy Directive 65-2, *Enterprise Risk Management and Managers' Internal Control Program* 16 May 2016

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, 18 February 2014

AFI 65-301, *Financial Management Internal Audit Services,* 31 August 2018

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* 6 February 2020

Air Force Instruction 33-360, *Publications and Forms Management*, 1 December 2015

AFI 33-322, *Records Management and Information Governance Program."* AFI 33-322 superseded AFMAN 33-363 use issuance date, 23 March 2020

AFI 36-1001 *Managing Civilian Performance Plans*, 8 November 2017

AFI 38-401, *Continuous Process Improvement,* 23 August 2019

AFI 90-802, *Operational Risk Management,* 1 April 2019

AFI 90-2001, *Mission Sustainment,* 31 July 2019

Air Force *Deficiency Acceptance and Corrective Action Plan Process Guide*

Air Force *Statement of Assurance Handbook*

SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015

SSAE No. 18, *Attestation Standards: Clarification and Recodification*, March 2018

Abbreviations and Acronyms list

AFPD—Air force Policy Directive

DCMO—Deputy Chief Management Officer

DoD—Department of Defense

DoDI—Department of Defense Instruction

ERM—Enterprise Risk Management

FFMIA—Federal Financial Management Improvement Act

FMR—Financial Management Regulation

FRDAA—Fraud Reduction and Data Analytics Act of 2015

GAO—Government Accounting Office

No.—Number

ODCFO—Office of the Deputy Chief Financial Officer

OMB—Office of Management and Budget

OUSD—Office of the Under Secretary of Defense

PL—Public Law

SSAE—Statement on Standards for Attestation Engagements

SP—Special Publication

TFM—Treasury Financial Manual

USSGL—United States Standard General Ledger

Vol—Volume

Prescribed Forms

No forms are prescribed by this publication.

Adopted Forms

Air Force Form 847, *Recommendation for Change of Publication*

Terms

Assessable Unit—The basic segment for which internal controls are evaluated. An assessable unit is a programmatic or organizational subdivision capable of being evaluated by internal control assessment procedures. An assessable unit shall be of an appropriate size to ensure the assessable unit manager has a reasonable span of control over its internal controls.

Assessable Unit Administrator—Administers the Managers' Internal Control Program within their assessable unit.

Assessable Unit Manager—The assessable unit manager is the principal manager or head of the assessable unit with authority and responsibility over the internal controls of the assessable unit.

Control Deficiency—A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to satisfactorily accomplish their assigned functions or inhibits the prevention or detection of misstatements on a timely basis.

Internal Control—The organization, policies, procedures, and instructions adopted by management to reasonably ensure mission or operational objectives are met, and programs achieve intended results, and to help managers safeguard the integrity of their programs. The concept of internal control applies to all Air Force activities.

Internal Control Assessment—A documented review performed by an AU to determine whether internal control techniques are effectively implemented to accomplish administrative, operational, and mission objectives.

Internal Control over Reporting—Provides an explicit level of assurance on the effectiveness of internal controls over financial reporting for each financial statement reporting entity. The assurance shall be based on the results of management's assessment conducted according to the requirements of OMB Circular No. A-123 Appendix A and the internal control over reporting guidance.

Internal Control over Financial Systems—Provides an explicit level of assurance on the effectiveness of internal controls over financial systems. The assurance shall be based on the results of management's assessment conducted in accordance with the requirements of OMB Circular No. A-123 Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996.

Internal Control over Operations—Provides an explicit level of assurance on the effectiveness and efficiency of operations for each entity as it pertains to the overall program, operational, and the administrative controls relevant to all mission-essential functions. The assurance shall be based on the results of management's assessment conducted according to the requirements of OMB Circular No. A-123 and the GAO Green Book.

Managers' Internal Control Program—The formal effort of an organization to ensure that internal control systems are working effectively through assignment of responsibilities at the policy level, issuance and implementation of guidance, conduct of internal control assessments, and reporting to senior management.

Management Control Plan—A written plan that details the assessable unit's inventory and is updated annually. The inventory will be maintained in the Management Control Plan and used to monitor progress and ensure that planned actions are taken. It must include at a minimum: 1) number of assessable units, 2) title of each assessable unit, 3) responsible assessable unit managers, 4) date of last Management Control Plan review 5) responsible Assessable Unit Administrator, 6) status of assessable unit manager training, 7) material weakness and significant deficiency, if reported, and 8) corrective action plan.

Material Weakness for Internal Control over Reporting—A significant deficiency or combination of conditions that adversely affects the entity's ability to initiate, authorize, record, process, or report external financial data reliably and according to generally accepted accounting principles. The condition creates more than a remote likelihood that a misstatement of the entity's financial statements, or other significant financial reports, is more than inconsequential and will not be prevented or detected.

Material Weakness for Internal Control over Financial Systems—The Air Force integrated financial management system is not in conformance with the Federal system requirements.

Material Weakness for Internal Control over Operations—A significant deficiency that the Department of Defense Component Head deems significant enough to report to a higher level. It is management's judgment as to whether or not a weakness is deemed material.

Primary Reporting Element—All major commands, the Air Force Operational Test and Evaluation Center, United States Air Force Academy, Air Force District of Washington, Air National Guard and Army Air Force Exchange Service are designated primary reporting elements of the Managers' Internal Control Program. SAF/FM will report directly to the Secretary of the Air Force. Resource Directorate, Office of Administrative Assistant to the Secretary of the Air Force (SAF/AAR) serves as the primary reporting element for all Secretariat and Air Staff offices. The heads of these organizations are the assessable unit managers who direct the Managers' Internal Control Program within their organizations.

Program Administrator—Form the Managers' Internal Control Program focal point network. The Program Administrator prepares and maintains the Primary Reporting Units' MCP.

Reasonable Assurance—An informed judgment, based upon an evaluation of all available information that the organization's systems of internal control are operating in a manner that achieves the objectives of the Federal Managers' Financial Integrity Act.

Significant deficiency—A control deficiency or combination of control deficiencies, that in management's judgment represents significant deficiencies in the design or operation of internal controls that could adversely affect the organizations ability to meet its internal control objectives, also known as a significant deficiency.

Senior Assessment Team—A team of senior level executives to provide oversight of assessing and documenting the effectiveness of internal controls and Federal Managers' Financial Integrity Act internal control over reporting and internal control over financial systems.

Statement of Assurance—An annual assessment in prescribed format that provides leader's explicit level of assurance on whether the internal controls are effective. The statement of assurance is a self-assessment conducted for mission-essential functions relative to risk and identifies any material weaknesses found.

Manager—A person responsible for controlling or administering all or part of the Air Force or assessable unit.

Entity—Entity in the context of Entity Level Controls refers to the Air Force as a whole.

Maturity Model—Outlines key indicators and activities that comprise a sustainable, repeatable and mature enterprise risk management (ERM) program.

Risk Taxonomy—Is a comprehensive listing of all potential categories and sub-categories of risk that should be considered when conducting a risk assessment. The risk taxonomy is designed to help identify risks across mission operations, business operations, governance, and information, and helps ensure the Air Force conducts a comprehensive assessment in line with OMB Circular A-123 requirements and OUSD guidance."

Attachment 2

REPORTING CATEGORIES

A2.1. Operational and Administrative Reporting Categories. Internal control deficiencies identified in the assessable unit's Management Control Plan and internal control accomplishments reported in the Statement of Assurance will be classified using the following categories:

A2.1.1. Communications. Communication requires a sender, message, and intended recipient, although the receiver need not be present or aware of the sender's intent to communicate at the time of communication; thus, communication can occur across vast distances in time and space.

A2.1.2. Intelligence. The plans, operations, systems, and management activities for accomplishing the collection, analysis, processing, and dissemination of intelligence in order to provide guidance and direction to commanders in support of their decisions.

A2.1.3. Security. The plans, operations, systems, and management activities for safeguarding classified resources (not peripheral assets and support functions covered by other reporting categories). Also covers Department of Defense programs for protection of classified information.

A2.1.4. Comptroller and Resource Management. Covers the budget process, finance and accounting, cost analysis, productivity and management improvement, and the general allocation and continuing evaluation of available resources to accomplish mission objectives. Includes pay and allowances for all Department of Defense personnel and all financial management areas not covered by other reporting categories, such as financial reporting.

A2.1.5. Contract Administration. The fulfillment of contractual requirements including performance and delivery, quality control and testing to meet specifications, performance acceptance, billing and payment controls, justification for contractual amendments, and actions to protect the best interests of the government.

A2.1.6. Force Readiness. The operational readiness capability of combat and combat support (both Active, Reserve, and Guard) forces which provide the necessary flexibility to deter potential foes and rapidly respond to a broad spectrum of global threats.

A2.1.7. Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes computers, ancillary equipment, software, firmware and similar services and related resources whether performed by in-house, contractor, or other intra-agency or intergovernmental agency resources or personnel.

A2.1.8. Acquisition. Acquisitions including major acquisitions and items designated as major systems that are subject to the procedures of the Defense Acquisition Board, the Military Services acquisition review councils, or the Selected Acquisition Reporting System. The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Guidance on the Assessment of Acquisition Functions under OMB Circular No. A-123," April 6, 2009 requires the use of an acquisition assessment template when

conducting internal control reviews and reporting material weaknesses for this category. Department of Defense Directive 5000.1 may be helpful when evaluating a weakness for inclusion in this category.

A2.1.9. Manufacturing, Maintenance, and Repair. The management and operation of in-house and contractor-operated facilities, performing maintenance and repair or installation of, modifications to materiel, equipment, and supplies. Includes depot and arsenal-type facilities as well as intermediate and unit levels of military organizations.

A2.1.10. Other. All functional responsibilities not represented by any other functional category, including management and use of land, sea, and air transportation for movement of personnel, materiel, supplies, and equipment using both military and civilian sources.

A2.1.11. Personnel and Organization Management. Authorizations, recruitment, training, assignment, use, development, and management of military and civilian Department of Defense personnel. Also includes the operations of headquarters organizations. Contract personnel are not covered by this category.

A2.1.12. Procurement. The decisions to purchase items and services with certain actions to award and amend contracts, e.g., contractual provisions, type of contract, invitation to bid, independent government cost estimate, technical specifications, evaluation and selection process, pricing, and reporting.

A2.1.13. Property Management. Construction, rehabilitation, modernization, expansion, improvement, management, and control over real property (both military and civil works construction) to include installed equipment and personal property. Also covers disposal actions for all materiel, equipment, and supplies including the Defense Re-utilization and Marketing System.

A2.1.14. Research, Development, Test, and Evaluation. The basic project definition, approval, and transition from basic research through development, test, and evaluation and all Department of Defense and contractor operations involved in accomplishing the project work. Excludes the support functions covered in separate reporting categories such as Procurement and Contract Administration.

A2.1.15. Security Assistance. Management of Department of Defense Foreign Military Sales, Grant Aid, and International Military Education and Training Programs.

A2.1.16. Supply Operations. The supply operations at the wholesale (depot and inventory control point) level from the initial determination of material requirements through receipt, storage, issue reporting, and inventory control (excluding the procurement of materials and supplies). Also covers all supply operations at retail (customer) level, including the accountability and control for supplies and equipment of all commodities in the supply accounts of all units and organizations (excluding the procurement of material, equipment, and supplies).

A2.1.17. Support Services. All support service functions financed from appropriated funds not covered by the other reporting categories, such as health care, veterinary care, and legal and public affairs services. All non-appropriated fund activities are also covered by this category.

A2.2. Financial Reporting and Financial System Reporting Categories. Financial reporting and financial system material weakness will be classified by one of the following end-to-end business process categories:

A2.2.1. Budget-to-Report. Encompasses the business functions necessary to plan, formulate, create, execute, and report on the budget and business activities of the entity. It includes updates to the general ledger. It also includes all activities associated with generating and managing the internal and external financial reporting requirements of the entity, including pre- and post-closing entries related to adjustments, reconciliations, consolidations, eliminations, etc.

A2.2.2. Hire-to-Retire. Encompasses the business functions necessary to plan for, hire, develop, assign, sustain, and separate personnel in the Department of Defense and Office of the Secretary of Defense Component.

A2.2.3. Order-to-Cash. Encompasses the business functions necessary to accept and process customer orders for services or inventory. This includes managing customers, accepting orders, prioritizing and fulfilling orders, distribution, managing receivables, and managing cash collections.

A2.2.4. Procure-to-Pay. Encompasses the business functions necessary to obtain goods and services. This includes requirements identification, sourcing, contract management, purchasing, payment management, and receipt and debt management.

A2.2.5. Acquire-to-Retire. Encompasses the business functions necessary to obtain, manage, and dispose of accountable and reportable property (capitalized and non-capitalized assets) through their entire life cycle. It includes functions such as requirements identification, sourcing, contract management, purchasing, payment management, general property, plant and equipment management, and retirement.

A2.2.6. Plan-to-Stock. Encompasses the business functions necessary to plan, procure, produce, inventory, and stock materials used both in operations and maintenance as well as for sale.