



DEPARTMENT OF DEFENSE
Defense Contract Management Agency

INSTRUCTION

Managers' Internal Control Program

Financial and Business Operations
OPR: DCMA-FBP

DCMA-INST 710
April 21, 2014

1. PURPOSE. This Instruction:

a. Reissues DCMA Instruction DCMA-INST 710 (Reference (a)) to update policy in accordance with DoD Directive (DoDD) 5118.03, "Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer" (Reference (b)); DoD Instruction (DoDI) 5010.40, "Managers' Internal Control Program (MICP) Procedures" (Reference (c)); Sections 1101 and 3512 (The Federal Managers' Financial Integrity Act) of Title 31, United States Code (U.S.C.) (Reference (d)); and Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Internal Control" (Reference (e)).

b. Establishes policy, assigns responsibility, and prescribes procedures for the execution of the MICP.

c. Establishes a formal mechanism for reporting the Agency annual Statement of Assurance (SOA) to the USD(C).

d. Is established in accordance with the authority in DoDD 5105.64, "Defense Contract Management Agency (DCMA)" (Reference (f)).

2. APPLICABILITY. This Instruction applies to all organizational elements of DCMA.

3. MANAGERS' INTERNAL CONTROL PROGRAM. In accordance with the Managers' Internal Control Program, this Instruction is subject to evaluation and testing. The process flow is located at the Policy Resource page of this Instruction.

4. RELEASABILITY – UNLIMITED. This Instruction is approved for public release.

5. PLAS CODE.

a. Processes: During documentation (narrative flow, and controls) or testing of a specific process; charge to the primary process; for general/administrative type support of the MICP and member participation in the Oversight Panel – Managers' Internal Control, charge 011 Management Control and Assessment Process.

- b. Programs: Acquisition Category/Other Customers (when applicable).
- c. Other National; Training and Travel; Local Programs (when applicable).
 - MICPEXC – Execution (Documenting narratives, flows and controls, AU inventories, process inventories, and corrective action plans (CAPs)).
 - MICPAST – Assessment (Documenting assessment of materiality and risk, and processes (e.g., process assessment, process testing, process review, management control reviews).
 - MICPRPT – Reporting (Reporting status of fiscal year plans, CAPs, AU certifications, Agency statement of assurance).

6. POLICY RESOURCE WEB PAGE. <https://home.dema.mil/policy/710r>

7. EFFECTIVE DATE. By order of the Director, DCMA, this Instruction is effective April 21, 2014, and all applicable activities shall be fully compliant within 60 days from this date.



Pamela F. Conklin
Executive Director
Financial & Business Operations/Comptroller

TABLE OF CONTENTS

REFERENCES	5
CHAPTER 1 – POLICY	
1.1. Policy	6
CHAPTER 2 – ROLES AND RESPONSIBILITIES	
2.1. DCMA Director or Principal Deputy.....	7
2.2. Senior Assessment Team (SAT).....	8
2.3. Resource Management Panel (RMP).....	8
2.4. Oversight Panel for MIC (OP-MIC).....	8
2.5. Agency MICP Coordinator	8
2.6. Assessable Unit Manager (AUM)/Sub-AUM.....	9
2.7. Assessable Unit Administrator (AUA)/Sub-AUA.....	10
2.8. All DCMA Employees.....	11
CHAPTER 3 – PROCEDURES	
3.1. Internal Controls (IC).....	12
3.2. Preparation of the Annual DCMA SOA	12
3.3. DCMA Assessable Units (AU).....	14
3.4. Senior Assessment Team (SAT).....	14
3.5. Reporting Period	14
3.6. Annual MICP Certification Statement.....	15
3.7. MICP Documentation Requirements	18
3.8. Inventory of AUs and Processes	18
3.9. MICP Plan.....	19
3.10. Risk Assessment Documentation.....	20
3.11. Control Assessment Documentation.....	24
3.12. Corrective Action Plans (CAP).....	26
3.13. Determining Materiality.....	27
3.14. MICP Reporting Categories.....	29
APPENDICES	
Appendix A Sample Info Memo.....	33
Appendix B Sample (Tab A) FY XXXX Accomplishments.....	34
Appendix C Sample (Tab B-1) List of all Uncorrected and Corrected Material Weakness – Reportable Conditions – Control Deficiencies	35
Appendix D Sample (Tab B-2) Uncorrected Material Weaknesses – Reportable Conditions – Control Deficiencies	36
Appendix E Sample (Tab B-3) Corrected Material Weaknesses – Reportable Conditions – Control Deficiencies	37

Appendix F	Sample of MICP Plan	38
FIGURES		
Figure 1	Risk Diagram.....	21
Figure 2	Sample Process Flow and Control Chart.....	23
TABLES		
Table 1	DCMA Assessable Units (AU).....	14
Table 2	Inventory of Assessable/Sub-Assessable Units	19
Table 3	Sample Inherent Risk Assessment.....	24
Table 4	Sample Control Assessment	26
Table 5	Sample Matrix of Materiality	28
GLOSSARY		
Definitions	40
Acronyms	44

REFERENCES

- (a) DCMA-INST 710, “Managers’ Internal Control Program,” September 11, 2011 (hereby canceled)
- (b) DoD Directive 5118.03, “Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer (CFO), DoD,” April 20, 2012
- (c) DoD Instruction 5010.40, “Managers’ Internal Control Program (MICP) Procedures,” May 30, 2013
- (d) Section 3512 of Title 31, United States Code
- (e) Office of Management and Budget Circular No. A-123, “Management’s Responsibility for Internal Control,” December 21, 2004
- (f) DoD Directive 5105.64, “Defense Contract Management Agency (DCMA),” January 10, 2013
- (g) DCMA-INST 973, “Performance Architecture,” February 10, 2014
- (h) Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, “Guidance on the Assessment of Acquisition Functions under Office of Management and Budget, Circular No. A-123,” April 6, 2009
- (i) Office of Management and Budget Memorandum, “Conducting Acquisition Assessments under Circular No. A-123,” May 21, 2008
- (j) Office of Management and Budget Circular No. A-127, “Financial Management Systems,” January 9, 2009
- (k) Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, “Financial Improvement and Audit Readiness Guidance,” current edition
- (l) Resource Management Panel Charter, March 25, 2011
- (m) Oversight Panel – Managers’ Internal Control Program Charter, March, 21, 2014
- (n) DCMA-INST 809, “Records Management,” May 1, 2009
- (o) Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense Memorandum, “Changes to the Annual ICOFR SOA Reporting Requirements,” April 22, 2011
- (p) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003, as amended

CHAPTER 1

POLICY

1.1. POLICY.

1.1.1. This Instruction implements DoD policy, pursuant to DoDI 5010.40 (Reference (c)), section 3512 of Title 31, U.S.C. (References (d)), and OMB Circular A-123 (Reference (e)), that a Managers' Internal Control Program (MICP) be established to review, assess, and report on the effectiveness of internal controls (IC) in DCMA. This DCMA Instruction shall establish and maintain a single, uniform program that DCMA components will use to develop, coordinate, assess, review, and publish reports pertaining to MICP.

1.1.2. Financial and Business Operations, as the primary process owner, shall oversee the development, implementation, administration, and management of the DCMA MICP.

1.1.3. Components are responsible for the effective and efficient implementation of processes within their functional areas, the reporting of IC practices, and adherence to the Agency's performance architecture, documented in DCMA-INST 973, "Performance Architecture" (Reference (g)) and the Agency strategic goals.

1.1.4. All processes must have a designated Assessable Unit Manager (AUM) who will develop, maintain, and report on effectiveness and efficiencies of their processes.

CHAPTER 2

ROLES AND RESPONSIBILITIES

2.1. DCMA DIRECTOR OR PRINCIPAL DEPUTY. The DCMA Director or Principal Deputy shall:

2.1.1. Establish a MICP to:

2.1.1.1. Assess inherent risks in mission-essential processes.

2.1.1.2. Document and design ICs.

2.1.1.3. Test the design and operating effectiveness of existing ICs.

2.1.2. Designate in writing the MICP Coordinator for the Agency within 90 days of a vacated position, and oversee the MICP Coordinator's implementation of procedures.

2.1.3. Conduct a formal assessment of the acquisition function requirements outlined in Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Memorandum (Reference (h)), and OMB Memorandum (Reference (i)) provide a summary of the assessment in the SOA.

2.1.4. Ensure critical elements related to MICP are developed and included in the performance plans for the senior accountable officials (i.e., AUMs and MICP Coordinator). (Sample: Instill a culture of accountability that promotes audit readiness throughout the directorate using effective ICs, process reengineering, enterprise resource planning, and financial reporting. Identify and promptly correct ineffective ICs within the directorate, ensuring that 95 percent of the milestones identified in the annual SOA for material weaknesses associated specifically with directorate processes are accomplished on schedule).

2.1.5. Submit the annual SOA to the Secretary of Defense (SD) and provide an informational copy to the Director of Financial Improvement and Audit Readiness (FIAR). Provide separate explicit levels of assurance in a SOA for each of the following three IC assessments required:

2.1.5.1. Operational and administrative controls relevant to all mission-essential functions throughout the Agency, except financial reporting and financial systems.

2.1.5.2. Financial reporting functions as assessed under the oversight of the senior assessment team (SAT).

2.1.5.3. Integrated Financial Management Systems (IFMS) conformance with the federal requirements according to DoDI 5010.40 (Reference (c)), section 3512 of Title 31, U.S.C. (References (d)), OMB Circular A-123 (Reference (e)), OMB Circular A-127 (Reference (j)), and USD(C)/Chief Financial Officer, DoD (Reference (k)).

2.2. SENIOR ASSESSMENT TEAM (SAT). The DCMA Council serves as the Agency SAT and convenes, as necessary, to advise the Agency Director on IC matters, including:

- 2.2.1. Assessing and monitoring MICP efforts.
- 2.2.2. Providing oversight and accountability for MICP.
- 2.2.3. Identifying IC issues that merit reporting in the annual SOA.
- 2.2.4. Taking prompt and effective actions to correct any identified issues in DCMA ICs.

2.3. RESOURCE MANAGEMENT PANEL (RMP). The RMP shall serve as the senior forum that shall facilitate cross-coordination and provide informal, working-level coordination for IC priorities and reporting, in accordance with Resource Management Panel Charter (Reference (l)).

2.4. OVERSIGHT PANEL FOR MIC (OP-MIC). The OP-MIC serves as a working level advisory body and is the forum that shall facilitate working level cross-coordination during the development of MICP requirements for Agency processes, in accordance with Oversight Panel – Managers’ Internal Control Program Charter (Reference (m)).

2.5. AGENCY MICP COORDINATOR. The Agency MICP Coordinator shall:

2.5.1. Coordinate with AUMs to ensure proper documenting of end-to-end processes that support operational, administrative, system, and financial events to assess controls and improve efficiency in the Agency.

2.5.2. Identify best business practices and recommend to AUMs ways to improve the control documentation, enhance controls, eliminate inefficient controls, or implement new controls.

2.5.3. Ensure subject matter experts (SME) assess risks that may adversely affect the Agency mission or operations.

2.5.4. Ensure that the Agency Director and AUMs identify IC objectives based on risk assessments in order to support the Agency.

2.5.5. Assist in testing, as necessary, and validate conclusions provided by SMEs on the effectiveness of ICs.

2.5.6. Assist in identifying and classifying IC deficiencies based on evaluations conducted.

2.5.7. Ensure that identified efficiencies, best practices, or deficiencies are shared across the assessable units (AU) throughout the Agency, to ensure relevant information is available for use by the Agency AUMs.

2.5.8. Monitor and track control issues through completion of corrective actions.

2.5.9. Actively communicate with the SAT on corrective action plans (CAP) and the resolution status for all control deficiencies in the reporting categories identified in this policy.

2.5.10. Prepare the annual SOA based upon material weaknesses identified during current and prior fiscal years (FY).

2.5.11. Maintain MICP documentation (e.g., process flows and narratives, associated risk matrices, control objectives, control activities, and AUM certifications), in accordance with DCMA-INST 809, "Records Management" (Reference (n)).

2.5.12. Develop, implement, recommend, and/or conduct annual Agency MICP training.

2.6. ASSESSABLE UNIT MANGER (AUM)/SUB-AUM. The AUM/Subordinate AUM (Sub-AUM) is designated as the Executive Director, Director, or Commander of the identified AU/Subordinate AU (Sub-AU). (**NOTE:** The AUM/Sub-AUM must be a government employee or uniformed service member due to the inherently governmental nature of the work). The AUMs/Sub-AUMs shall:

2.6.1. Provide the Agency MICP Coordinator with a list of Sub-AUs and mission critical processes annually (Sub-AUM provides to AUM).

2.6.2. Assess risks that may adversely affect the AU's mission or operations.

2.6.3. Identify IC objectives that support the AU.

2.6.4. Document operational, administrative, system and financial ICs.

2.6.5. Review processes and procedures to provide recommendations for the enhancement, elimination, or implementation of AU ICs.

2.6.6. Recommend the retention, enhancement, elimination, or implementation of ICs for the AU.

2.6.7. Test the effectiveness of the ICs.

2.6.8. Identify and classify IC deficiencies according to the reporting categories described in paragraph 3.14 of this Instruction.

2.6.9. Develop CAPs.

2.6.10. Track progress of CAPs.

2.6.11. Actively communicate with the MICP Coordinator on CAPs as required for reporting and resolution of all control deficiencies.

2.6.12. Designate Sub-AUs and Sub-AUMs as appropriate for management of processes, and concur with the appointment of Subordinate Assessable Unit Administrators (Sub-AUA) by the Sub-AUM. Consideration shall be given to designating Centers, Regions, and Contract Management Offices. Ensure the addition of a critical element to the Individual Performance Plan (IPP) of the Sub-AUM that indicates the effective and timely resolution of the material and systemic issues associated with their Sub-AUs. (Sample: Instill a culture of accountability that promotes audit readiness using effective ICs, process reengineering, enterprise resource planning, and financial reporting. Identify and promptly correct ineffective ICs, ensuring that 95 percent of the applicable milestones identified in the annual SOA are accomplished on schedule.)

2.6.13. Appoint Assessable Unit Administrator (AUA)/Sub-AUA for the AU/Sub-AU. Ensure the addition of a critical element to the IPP of the AUA/Sub-AUA regarding the administration of MICP in the AU/Sub-AU. (Sample: Instill a culture of accountability that promotes audit readiness, in accordance with Agency MICP requirements; document all processes and associated risk, scheduled and unscheduled reviews, material weaknesses, control deficiencies, reportable conditions and CAPs. Ensure that MICP reporting requirements are met and that 95 percent of the applicable milestones identified, in the annual SOA, are accomplished on schedule.)

2.6.14. Annually provide an AU SOA certification with explicit level of assurance, to the Agency Director via the Agency MICP Coordinator to support the Agency SOA.

2.6.15. Maintain MICP documentation (e.g., process flows and narratives, associated risk matrices, control objectives, control activities, and AUM certifications) in a central location to efficiently provide documents to the MICP Coordinator as requested. Some documentation may exist for other purposes, including operating instructions, standard operating procedures, or other policy directives.

2.7. ASSESSABLE UNIT ADMINISTRATOR (AUA)/SUB-AUA. The AUA/Sub-AUA shall:

2.7.1. Assist the AUM/Sub-AUM in the implementation of the MICP.

2.7.2. Consolidate and prepare the annual AU certification to the Agency SOA based on internal findings on effectiveness of the ICs over AU/Sub-AU operations, financial, and systems requirements, identifying the AU/Sub-AU's level of reasonable assurance of the effectiveness of ICs; coordinate draft report; submit via each leader's next higher level of authority to the AUM for approval for coordination with the Agency MICP Coordinator.

2.7.3. Monitor and consolidate the Quarterly Reports of Corrective Milestones to Agency MICP Coordinator.

2.7.4. Identify and coordinate MICP training requirements for the AU.

2.7.5. Represent their respective AU, as well as the best interests of the Agency, by actively participating in the OP-MIC meetings.

2.8. ALL DCMA EMPLOYEES. All DCMA employees, civilian and military, are responsible to reasonably assure that programs achieve their intended results; risk of loss of life and/or loss of public trust is mitigated; the use of resources is consistent with the Agency's mission; programs and resources are protected from waste, fraud, and abuse; laws and regulations are followed; and that reliable and timely information is obtained, maintained, reported, and used for decision making.

CHAPTER 3

PROCEDURES

3.1. INTERNAL CONTROLS (IC). ICs are sound management practices and play an important role in achieving business and mission objectives throughout DCMA. AUMs/Sub-AUMs should not be encumbered by controls but rather benefit from them. AUMs/Sub-AUMs must ensure an appropriate balance between too many and too few controls.

3.1.1. DoDI 5010.40 (Reference (c)) provides the DoD Instruction on establishing a MICP, which is comprised of the Federal Manager's Financial Integrity Act (FMFIA) internal control over nonfinancial operations (ICONO), internal control over financial reporting (ICOFR), and internal control over financial systems (ICOFS). DoD policy commands that agencies establish a MICP to evaluate and report on the effectiveness of ICs throughout the agency and make corrections when necessary. AUs shall use the USD(AT&L) Memorandum (Reference (h)), as required, along with organizational assessments, evaluations, and other contributing information (e.g., performance metrics, external audits and inspections, etc.) as forms of monitoring ICs.

3.1.2. MICP shall encompass the Government Accountability Office's (GAO) five standards for IC: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communications, and (5) monitoring. The design, operations, and documentation of the agency's programs should provide reasonable assurance that the objectives detailed in DoDD 5118.03, (Reference (b)); DoDI 5010.40 (Reference (c)); section 3512 of Title 31, U.S.C. (Reference (d)) are met.

3.1.3. AUMs/Sub-AUMs shall implement a system of ICs to provide reasonable assurance that the following objectives are met:

3.1.3.1. Effectiveness and efficiency of operation.

3.1.3.2. Reliability of financial reporting.

3.1.3.3. Compliance with applicable laws and regulations.

3.1.4. Implementation of this program should not duplicate existing control efforts, but rather complement other efforts (e.g., Financial Improvement Program, DCMA Safety Program, performance appraisal processes, etc.).

3.2. PREPARATION OF THE ANNUAL DCMA SOA.

3.2.1. DCMA is responsible for preparing and compiling the annual SOA and submitting it to the Under Secretary of Defense (Comptroller) (USD(C)), via the Under Secretary of Defense, Acquisition, Technology and Logistics (USD(AT&L)). This responsibility is delegated to the Agency MICP Coordinator. Information regarding ICs, to include both control deficiencies and control-related accomplishments, is collected through two main venues: self-reporting and audits. AUs are represented by DCMA components. AUMs review IC certification statements

from their subordinate units, and in turn submit certification statements to the Agency Director via the Agency MICP Coordinator. This “self-reporting” of control deficiencies enables the AUMs to demonstrate their control environments and activities, and to indicate the findings of their control assessments. Complementing the self-reporting of control deficiencies, the AUMs use external audit reports (GAO, DoD Inspector General (IG), National Aeronautics and Space Administration, Special IG, etc.), internal audit reports (Mission Review Team (MRT), Internal Review Team (IRT), bell ringer reporting, etc.), performance reviews, input from Continuous Process Improvement and Lean Six Sigma to help identify material control deficiencies throughout the year. AUMs/Sub-AUMs will work closely with the MRT and IRT to review audit reports on a quarterly basis and utilize a systemic method to determine materiality and potential inclusion into the annual SOA.

3.2.2. AUMs shall work to develop, document, and monitor corrective actions and milestones in accordance with DoDI 5010.40 (Reference (c)) and applicable annual guidance for both self-reported issues and those stemming from audit reports or other sources. The Agency MICP Coordinator must reference any DCMA “Systemic Weaknesses” identified by the AUMs during the MICP Certification Process and report material weaknesses in the Agency SOA.

3.2.3. The annual SOA includes a separate certification on ICONO, ICOFR, and ICOFS as applicable based upon the MICP annual guidance.

3.2.3.1. Operations Assessment. IC deficiencies, (material weaknesses, reportable conditions, or control deficiencies) based on testing design and operation, will be reported in the AUM certification to the Agency SOA to the SD. The classification of IC deficiencies is management’s judgment. The concept of materiality is not primarily financial. Qualitative factors such as impact on mission success or failure, health and safety, and threat to image must be considered. DCMA will conduct an assessment of the acquisition functions for major defense acquisition programs through a process consistent with the guidance contained in OMB Memorandum (Reference (i)). This process includes completing the DoD Assessment of ICs over Acquisition Functions Template, determining if there are acquisition function control deficiencies, summarizing the results of the completed assessment, and developing a CAP(s), if necessary, for reporting into the SOA. The guidance in USD(AT&L) Memorandum (Reference (h)) applies to all acquisitions, including major acquisitions and items designated as major systems, subject to the procedures of the Defense Acquisition Board, the Military Services Acquisition Review Councils, or the Selected Acquisitions Reporting System.

3.2.3.2. Financial Reporting Assessment. AUs will use the methodology in the FIAR guidance, USD(C)/Chief Financial Officer, Department of Defense (Reference (k)), to identify deficiencies within end-to-end business processes. The Agency will develop a financial improvement plan that incorporates CAPs for IC deficiencies identified, as required by DoDI 5010.40 (References (c)) and USD(C)/Chief Financial Officer, Department of Defense (Reference (k)). Summaries of the CAPs will be reported in accordance with USD(C)/Chief Financial Officer, Department of Defense Memorandum (Reference (o)).

3.2.3.3. Financial Systems Assessment. AUs will use the methodology in the FIAR guidance to assess, evaluate, and report the conformance of their IFMS compliance with federal

requirements prescribed in DoDI 5010.40 (References (c)), section 3512 of Title 31, U.S.C. (Reference (d)), and OMB Circular A-127 (Reference (j)). Nonconformance with federal financial management system requirements constitutes a material weakness, which must be reported in the SOA and accompanied by CAP summaries with the milestones for resolution. The Agency’s portion of the IFMS designated as the role of service providers must provide testing of material controls within the IFMS by an auditor as part of the service provider agreement to enable the Agency to assess the reliability of the overall IFMS in accordance with USD(C)/Chief Financial Officer, Department of Defense (Reference (k)).

3.3. DCMA ASSESSABLE UNITS (AU). AUs represent all DCMA components that report directly to the Agency Director. The component head of each AU has the responsibility and accountability for establishing and assessing ICs.

Table 1. DCMA Assessable Units (AU)

Aircraft Operations Executive Directorate	AO
Contracts Executive Directorate	AQ
Office of the Chief of Staff	DC
Office of Independent Assessment	DM
Office of Reserve Affairs	DR
Corporate Support Executive Directorate	DS
Engineering and Analysis Executive Directorate	EA
Financial and Business Operations Executive Directorate	FB
Office of General Counsel	GC
Human Capital Executive Directorate	HC
Information Technology Executive Directorate	IT
Portfolio Management and Integration Executive Directorate	PI
Quality Assurance Executive Directorate	QA
International Directorate	I
Special Programs Directorate	S
Operations Directorate	O

3.4. SENIOR ASSESSMENT TEAM (SAT). The SAT will meet at least twice annually to discuss progress on reported material weaknesses, reportable conditions, and control deficiencies as well as potential new material weaknesses, reportable conditions, and/or control deficiencies.

3.5. REPORTING PERIOD.

3.5.1. The DCMA SOA reporting period follows the October 1 to September 30 FY.

3.5.2. Since the preparation of the DCMA SOA occurs during the fourth quarter (QTR) of the FY, it is strongly advised to not assign milestones to the fourth QTR (July – September). It is difficult to accurately report on and update fourth QTR milestones once the preparation of the DCMA SOA begins. For this reason, if a milestone is scheduled to be completed on August 1st in the current FY, identify the targeted completion date of the milestone as the first QTR of next FY. This will allow adequate time to confirm the completion of the milestone and report via each

leader's next higher level of authority to the AUM for approval and coordination with the Agency MICP Coordinator.

3.6. ANNUAL MICP CERTIFICATION STATEMENT.

3.6.1. Submitting Instructions. All DCMA AUMs are required to provide input to the annual DCMA SOA by submitting an MICP Certification Statement. Signed Certification Statements, along with supporting enclosures, will be submitted (electronically via e-mail) to the Agency MICP Coordinator no later than June 15th.

3.6.2. Preparing a MICP Certification Statement. The submission of the MICP Certification Statement shall include:

3.6.2.1. Info Memorandum. An info memorandum, addressed to the Agency MICP Coordinator and signed by the AUM, shall provide the AUM's assessment as to whether there is reasonable assurance that ICs are in place and operating effectively. Appendix A provides a sample info memorandum. The certification must take one of the following three forms:

3.6.2.1.1. An unqualified SOA (reasonable assurance with no material weaknesses reported). Each unqualified statement should describe how the level of assurance is supported and how assessments were conducted.

3.6.2.1.2. A qualified SOA (reasonable assurance with the exception of one or more control issue(s) noted or the IFMS is not in conformance with federal requirements). The cover memorandum must cite the material weakness(es) in ICs that preclude an unqualified statement. Tab B-2 will fully describe all weaknesses, the corrective actions being taken and by whom, and the projected QTR and FY of those corrective actions.

3.6.2.1.3. A statement of no assurance (no reasonable assurance because few or no assessments were conducted or the noted material weaknesses are pervasive across many key operations or the IFMS is substantially noncompliant with federal requirements). The AUM shall provide an extensive rationale for this position.

3.6.2.1.4. The AUM must certify to the number of IC assessments that were scheduled for the reported MICP year.

3.6.2.2. Tab A: Accomplishments. Tab A shall include a brief summary of the most significant accomplishments and actions taken by the AUM during the current FY to strengthen ICs. The accomplishments shall be ordered by significance with most significant accomplishment listed first. Appendix B provides a sample of Tab A, Accomplishments.

3.6.2.3. Tab B-1: List of All Uncorrected and Corrected Material Weaknesses - Reportable Conditions - Control Deficiencies. Tab B-1 shall serve as a table of contents and listing of the titles of all uncorrected and corrected Material Weaknesses, Control Deficiencies, and Reportable Conditions. Appendix C provides a sample of (Tab B-1) List of all Uncorrected and Corrected Material Weaknesses - Control Deficiencies - Reportable Conditions.

3.6.2.4. Tab B-2: Uncorrected Material Weaknesses - Reportable Conditions - Control Deficiencies. Tab B-2 will be completed for each uncorrected Material Weakness, Reportable Condition, and Control Deficiency and shall contain detailed narrative descriptions, including the plans and schedules for the corrective action(s). Include a separate form for each Material Weakness, Reportable Condition, and Control Deficiency identified during the current year and those disclosed in prior years with updated information.

3.6.2.4.1. The narrative shall be in the format provided in Appendix D and shall include the following data elements:

3.6.2.4.1.1. Date Identified. Date the issue was identified.

3.6.2.4.1.2. Issue Type. Document whether the issue is a Material Weakness, Reportable Condition or Control Deficiency.

3.6.2.4.1.3. Title. Provide a specific title that narrowly defines the issue. Do not use broad categories to title specific issues. Confine the issue description to three sentences if possible.

3.6.2.4.1.4. Associated Program or Process. Indicate the program or process associated with the issue, which must match the Agency Process Inventory.

3.6.2.4.1.5. Functional Category. Indicate one of the functional categories that are described in paragraph 3.14. titled "MICP Reporting Categories" in this Instruction, e.g., "Force Readiness" must match the Agency Process Inventory.

3.6.2.4.1.6. Line of Service. Indicate the line(s) of service associated with the issue, must match the Agency Process Inventory.

3.6.2.4.1.7. Created By. Name and component of employee identifying the issue.

3.6.2.4.1.8. Component with Primary Responsibility (CPR) SME. Identify the SME documented on the Agency Process Inventory as responsible for Agency implementation of the program or process identified.

3.6.2.4.1.9. Assessable Unit Manager. Name and title of the AUM in charge of ensuring this weakness is resolved according to the proposed CAP, must match the Agency Process Inventory.

3.6.2.4.1.10. Year Identified. FY of the annual certification statement in which the AUM first reported the weakness.

3.6.2.4.1.11. Original Targeted Correction Date. The QTR and FY of the targeted correction date as first reported by the AUM. (For all targeted correction dates, AUMs must show both the QTR and FY; e.g., 1st QTR FY 2013).

3.6.2.4.1.12. Targeted Correction Date in Last Year's Report. QTR and FY of the targeted correction date as the AUM reported in the AU's annual MICP Certification Statement for the previous year. If this is a new weakness, indicate "N/A" (not applicable).

3.6.2.4.1.13. Current Target Date. QTR and FY of current targeted correction date.

3.6.2.4.1.14. Reason for Change in Date. Document justification for the change from the last target date; if competing priorities are the reason, those priorities must be detailed in the justification.

3.6.2.4.1.15. Description of Issue. Narrative describing the issue.

3.6.2.4.1.16. Significance of Issue. Documentation of the magnitude of resources (people, time, money) that are affected by this issue.

3.6.2.4.1.17. Source(s) Identifying Issue. Identify how the issue was identified. (MICP evaluation; external audit (specify); internal audit (specify); AUM internal review; or other (specify)). When audit findings are the source of weakness identification, identify the title, number, and date of the document in which the weakness was identified. If the weakness was identified by more than one source, list all identifying sources in order of significance.

3.6.2.4.1.18. Results Indicator. Identify the measure that will be used to ensure the issue does not recur. Measures must be quantitative and/or qualitative measures that determine the benefits derived or to be derived from the corrective action and the overall impact of the correction on operations. If monetary benefits can be determined, state that information here. **NOTE:** Specifically identify one or two defined performance measures, metrics, or results that will be used to determine the successful completion of the proposed remedial effort.

3.6.2.4.1.19. Validation Process. Identify the methodology and actions that will be taken to confirm that the issue is resolved to certify the effectiveness of the corrective action(s).

3.6.2.4.1.20. Milestones. Identify the action(s) taken to correct the issue. Separate milestones into two categories: Completed Milestones (Progress to Date) and Planned Milestones. List major milestones in chronological order by milestone completion date with the terminal milestone listed last. The terminal milestone is the final corrective action and should include validation that the weakness is corrected.

3.6.2.4.2. General rules to follow when completing Tab B-2:

3.6.2.4.2.1. Do not exclude sections, if they are not applicable, note "N/A."

3.6.2.4.2.2. Spell out acronyms the first time they are used in each individual material weakness narrative.

3.6.2.4.2.3. Narratives should be succinct, void of technical jargon, and easy for the general public to interpret.

3.6.2.5. Tab B-3: Corrected Material Weaknesses, Reportable Conditions, and Control Deficiencies. Tab B-3 will be completed for each corrected Material Weakness, Reportable Condition, and Control Deficiency, and shall contain detailed narrative descriptions, including the most significant actions taken to correct each weakness. This section will include all corrected weaknesses that were identified in either the current year or prior year. The data elements are similar to the data elements in Tab B-2. Follow the general rules for Tab B-2 when completing Tab B-3. For each corrected material weakness, the last completed milestone will describe the method used to validate the corrective action including a certification that the corrective action effectively resolved the weakness. Appendix E provides a sample of Tab B-3, Corrected Material Weaknesses, Reportable Conditions, and Control Deficiencies.

3.7. MICP DOCUMENTATION REQUIREMENTS.

3.7.1. DCMA MICP Coordinator must maintain the following MICP documentation for FMFIA Overall Process for access by all DCMA AUMs:

3.7.1.1. Inventory of Sub-AUs and Processes.

3.7.1.2. MICP Plan.

3.7.1.3. Materiality and Risk Assessments.

3.7.1.4. IC Assessments.

3.7.1.5. Corrective Actions for Control Deficiencies, Reportable Conditions, and Material Weaknesses.

3.8. INVENTORY OF AUs AND PROCESSES.

3.8.1. AUs are designed to provide a reasonable span of control to conduct MICP assessments of processes. A Sub-AU can be any organization, function, program, or subdivision capable of being evaluated using IC assessment procedures. A Sub-AU must have clear limits or boundaries and be identifiable to a specific responsible manager. Further, it must be small enough to provide reasonable assurance of adequate management controls but large enough that any detected material weakness has the potential to impact the mission of the Agency.

3.8.2. AUs must constitute the entire Agency. This means that every part of the Agency must be represented by one of the AUs in the Agency's inventory of AUs.

3.8.3. DCMA AUs are structured by organization. AUMs will identify Sub-AUs to better document process assessment or to better establish documentation of standard processes for AU mission execution. At a minimum, the Inventory of Assessable/Sub-Assessable Units (Table 2) shall include the name of the AU and responsible manager identified by name and title.

3.8.4. The AU’s inventory of Sub-AUs and the AU’s inventory of processes shall be updated at least annually to reflect changes within the AU.

NOTE: The following example is only a guide and is not intended to be replicated by every AUM. AUMs should use the format that is most conducive to the AU environment and organizational practices to document their Sub-AUs.

Table 2. Inventory of Assessable/Sub-Assessable Units

Inventory of Assessable/Sub-Assessable Units	
Assessable Unit: Financial & Business Operations Executive Directorate	
Sub-Assessable Unit Name	Sub-Assessable Unit Manager
1. Budget Operations	J. Doe, Director Financial Operations
2. Accounting Services	K. Smith, Director Financial Services
3. Financial Planning	A. King, Director Financial Planning
4. Manpower Operations	C. Jones, Director Manpower
5. Financial Systems	D. James, Director Financial Systems

3.9. MICP PLAN. The MICP Plan is an executive summary of each AUM’s MICP. The plan captures each AUM’s approach to implementing an effective IC program. The consolidation of each AUM’s plan serves as the first resource to the Agency’s MICP program.

3.9.1. The MICP Plan will assist in the transition from one AUM and AUA to another by establishing in writing how the AU is implementing the relevant guidance. New AUMs/AUAs shall use the MICP Plan to learn the specific approach and vision of MICP within their AUs.

3.9.2. The MICP plan shall be updated by the AUMs at least annually and forwarded to the Agency MICP Coordinator. Figure 1 and Appendix A can be used to create the AU MICP plan. The MICP plan process is provided on the resource page as a guide. The guide outlines the key information required for each AUM to provide assistance in developing a robust plan. The format presented in the guide is designed to meet the reporting requirements of the GAO’s five standards for IC. The plan may take any form but must identify the following key elements:

3.9.2.1. FY associated with the plan.

3.9.2.2. Identification of the AUA.

3.9.2.3. Overview of MICP within the AU addressing all five elements of the GAO standards: Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring.

3.9.2.4. Description of how accomplishments will be documented.

3.9.2.5. Description of how CAPs will be documented and monitored.

3.9.2.6. Schedule of documented training.

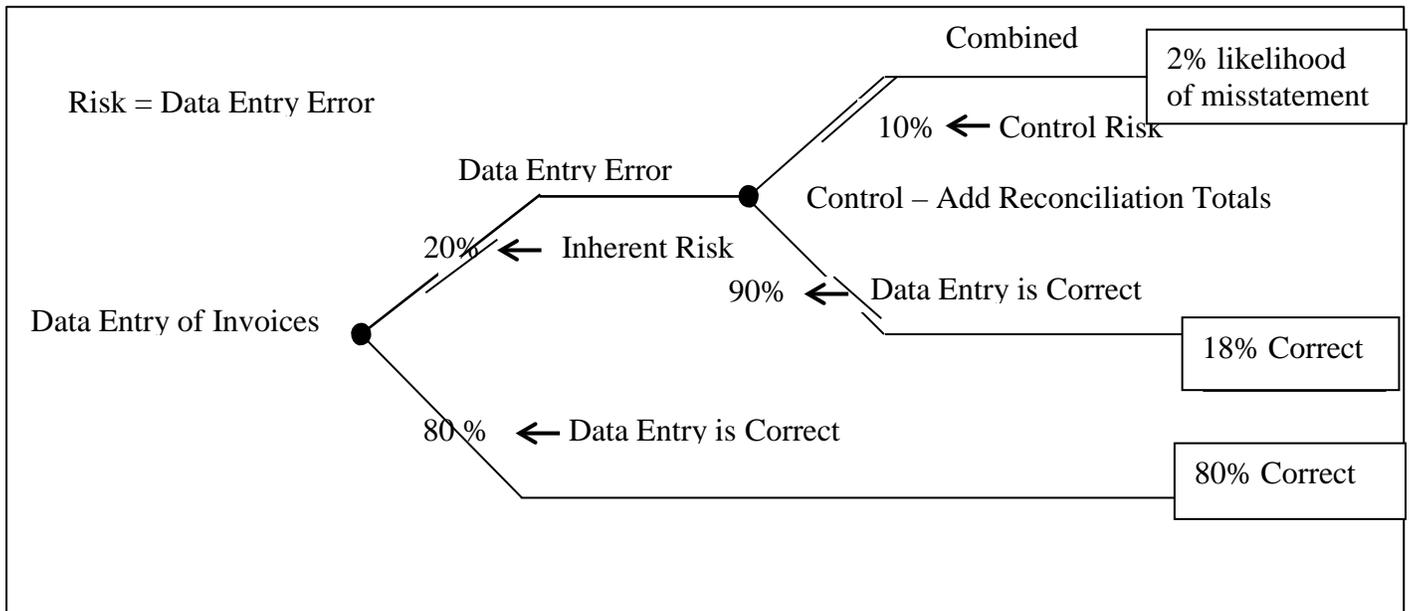
3.9.2.7. Description of what will be assessed (includes identification of all processes owned, the process risk rating, the process materiality rating, date of scheduled process review, and date of completion of process CAP (if applicable).)

3.10. RISK ASSESSMENT DOCUMENTATION. A risk assessment determines where a potential hazard exists that might prevent the Agency from achieving its objectives. Asking the following questions may help to define and identify risks in each process that the AU is responsible for:

- What could go wrong in the process?
- What processes require the most judgment?
- What processes are most complex?
- What must go right for proper reporting?
- How could we fail to report accurately?
- How do we know whether we are achieving our objectives?
- What are our vulnerable areas?

3.10.1. Each of the risks identified in a mission and/or business process, control activity, or combination of control activities should be identified and documented in the risk assessment. The GAO identifies three types of risk:

Figure 1. Risk Diagram



3.10.1.1. Inherent Risk. The original susceptibility to a potential hazard or material misstatement, assuming there are no related specific control activities. For example, human error in data entry of figures.

3.10.1.2. Control Risk. The risk that a hazard or misstatement will not be prevented or detected by the IC. For example, the control activity to prevent data entry error is to include a reconciliation total. The control to mitigate risk is that the reconciliation total will not prevent a misstatement.

3.10.1.3. Combined Risk. (Also known as residual risk) the likelihood that a hazard or material misstatement would occur and not be prevented or detected on a timely basis by the agency's IC. For example, combined risk remains if the transposition of numbers in the data entry process resulted in the total transactions matching the reconciliation total. In this case, the reconciliation total would not mitigate the inherent risk. The risk that remains is known as the combined risk.

3.10.2. Figure 1 is a risk diagram which illustrates how risk can be measured and demonstrates how that measurement can influence decision making. Percentages are used to distinguish the different risks, however, are not required when preparing the risk assessment.

3.10.3. While risk assessment documentation is required, there is no prescribed format for completing a risk assessment for the MICP overall. The goal is to maintain risk assessment documentation that gives managers the information they need to establish and improve ICs to provide reasonable assurance.

3.10.4. The Agency's risk assessment should be used to support daily management decisions.

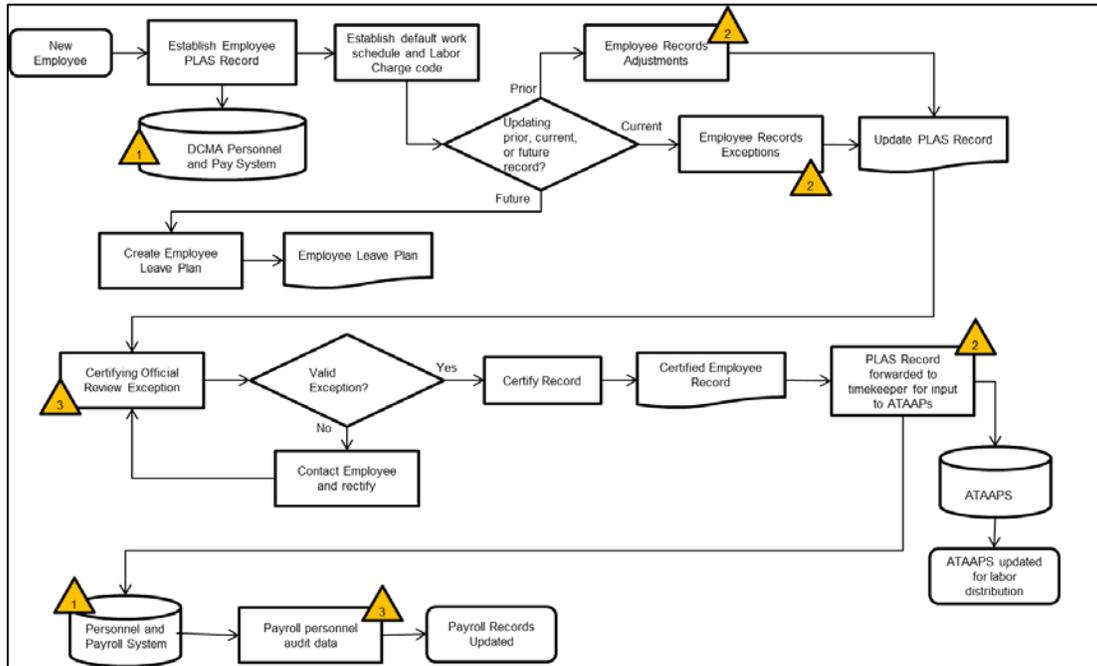
3.10.5. The following tools may assist in preparing risk assessment documentation:

3.10.5.1. Process Narrative and Process Flowchart. Preparing process narratives and process flowcharts that describe and illustrate the major and essential operations can assist in identifying risks and control deficiencies.

3.10.5.1.1. Process narratives are written descriptions of the flow charts, explaining what actions are being taken in each step. The process flowchart and controls (Figure 2) should complement the process narrative and summarize the significant steps in major and essential operations. Additionally, the method(s) of communication used to share the status of steps throughout the process can be documented.

3.10.5.1.2. The flowchart will identify key processes and their related control activities such as control over information processing, physical control over vulnerable assets, segregation of duties, and accurate and timely recording of transactions and events. These flowcharts can then be linked to the required risk assessment documentation.

Figure 2. Sample Process Flow and Control Chart



Key Control Table			
Control	Functional Area	Risk	Possible Control
1	Security	<ul style="list-style-type: none"> - Unauthorized access to sensitive data - Unauthorized access to sensitive DCMA data by payroll personnel 	<ul style="list-style-type: none"> - Clearly documented policies and procedures - Access restricted to very few individuals - Password security - Logging procedures - Restricted access and update capabilities
2	Documentation	<ul style="list-style-type: none"> - Unauthorized charges - Improper payment of overtime 	<ul style="list-style-type: none"> - Logging of all adjustments - Supervisory review of employee actual time worked - System edits to control payment of overtime to FLSA-exempt employees
3	Approval	<ul style="list-style-type: none"> - Non-accountability of additions/modifications - Unauthorized charges 	<ul style="list-style-type: none"> - Clearly documented policies - Access restricted to individual employee's own data - Strict password security - Digital signatures - Limited certification authority

3.10.5.2. Risk Assessment Table. Some form of a risk assessment table will be necessary to document the risk assessment. The following data elements are included in the Sample Risk Assessment (Table 3).

3.10.5.2.1. The numbers in the columns of the Risk Assessment Table correlate to the following instructions.

3.10.5.2.1.1. Identify all assessable processes.

3.10.5.2.1.2. Identify the criteria for assessing inherent risk. (The approach to this process of identifying risks is to envision what could go wrong. What problems could arise that might hinder the objective?)

3.10.5.2.1.3. Identify the level of Inherent Risk as High, Moderate, or Low. If inherent risk is determined to be “High”, stronger or more extensive controls to prevent or detect misstatements may be needed than if inherent risk is “Low”.

Table 3. Sample Inherent Risk Assessment

	(2)	(3)		
AU: DCMA FB	Risk Criteria	High (Rated 3)	Moderate (Rated 2)	Low (Rated 1)
	Cost	Over 1% of Agency Budget	Over 1% of AU Budget	Below 1% of AU Budget
	Agency Use	DCMA and Customer	DCMA	Directorate Only
	Reporting	Every Day	Once a Quarter	Once a Year
	The higher the number, the higher the inherent risk.			
Process (1)	Cost	Agency Use	Time	Total Inherent Risk
Time and Attendance	3	2	3	8
General Ledger Review	2	2	2	6
MICP	1	2	1	4

3.11. CONTROL ASSESSMENT DOCUMENTATION. Once ICs are in place, management is required to actively monitor those controls to ensure that they are functioning correctly and effectively, mitigating the associated risk. Control assessments can include both an internal review of controls and evaluations from external organizations such as audit organizations or offices of IG.

3.11.1. Every AU shall document assessment of their processes annually. The AUM of the AU is required to report each year in their MICP Certification Statement the number of completed IC assessments for the current MICP year, and the results of those assessments. The scope of the IC assessment is based on management’s judgment.

3.11.2. During the risk assessment of the process, individual documented controls will initially be rated as having a low, moderate, or high control risk. Usually a control would be rated high if the control has not been implemented or if the control is not effective in either design or operation. Spending time on testing an ineffective or high risk rated control is

counterproductive. Develop a CAP for all “high” risk rated controls to decrease the risk of vulnerability or failure within the process.

3.11.3. Controls with low or moderate control risk should be tested to see if the controls are effective. If the control is assessed to be ineffective, the control should be reclassified as having a high control risk. Develop CAPs for those controls that are reclassified as having a high control risk.

3.11.4. Significant control deficiencies should be reported to the Agency MICP Coordinator, via the next higher level of authority as either a reportable condition or material weakness, based on management judgment.

3.11.5. While IC assessment documentation is required, there is no prescribed format for completing an IC assessment for the MICP overall. The goal is to maintain IC assessment documentation that gives managers the information they need to establish and improve ICs within their AU.

3.11.6. Some form of an IC assessment table (Table 4) is necessary to document the IC assessments required.

3.11.7. The numbers in the columns of the IC Assessment Table correlate to the instructions below:

3.11.7.1. Identify the control test objective to validate the assumed level of control risk.

3.11.7.2. Describe the design of the control that will be tested.

3.11.7.3. Answer if the design of the control is effective based upon the testing performed (choose either “Yes” or “No”).

3.11.7.4. Describe how the control operation was tested.

3.11.7.5. Answer if the control operation is effective based upon the testing performed (choose either “Yes” or “No”).

3.11.7.6. Identify the new level of control (determine the new level of control risk based on the control design test and the control operation test.) For example, if the initial control risk was “Low” and was tested to be ineffective for both the design and control operation tests, the new control risk level would be elevated to “High.” However, if the initial control risk was “Low” and both the design and control operation tests were effective, the control risk level would stay classified as “Low.”

Table 4. Sample Control Assessment

Control Assessment								
AO/Sub-AU: DCMA FB								
Preparer: C Jones								
Process: Time and Attendance Process								
Control Number	Risk	Internal Control Currently In Place	(1) Control Test	(2) Description of Design Test	(3) Was Control Design Effective?	(4) Description of Control Operation Test	(5) Was Control Operation Effective?	(6) New Control Risk Level
1	Employee inaccurately records hours worked	Supervisor reviews employee's timesheets and approves hours worked	Ensure supervisors are accurately reviewing timesheets	Review existence of approved timesheets	Yes	Track employee's time and compare with approved timesheets	Yes	Low
2	Timekeeper could inaccurately input data into the T & A system	FB employee reviews his/her time account with timekeeper and signs / dates to verify that the information is accurate	Ensure the FB employee's review effectively reduces inaccuracies on recorded timesheets	Review existence of verification forms	Yes	Compare approved timesheets with timesheets recorded in the T & A system	Yes	Low

3.12. CORRECTIVE ACTION PLANS (CAP). Monitoring of ICs shall include policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved.

3.12.1. AUMs are to:

3.12.1.1. Promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate the Agency's operations.

3.12.1.2. Determine proper actions in response to findings and recommendations from audits and reviews.

3.12.1.3. Complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that corrects identified deficiencies, produces improvements, or demonstrates the findings and recommendations do not warrant management action.

3.12.2. CAPs for all material weaknesses, reportable conditions and control deficiencies shall be included as an enclosure to the MICP Certification Statement. Formatting instructions are outlined in paragraph 3.6. titled "Annual MICP Certification Statement" in this Instruction.

3.13. DETERMINING MATERIALITY. Materiality is a management judgment. It is difficult to apply a strict formula or test to determine whether something is or is not material. There are, however, important questions that can be asked to help management determine if an issue is a material weakness.

3.13.1. Is the issue control-related? Consider whether the issue is related to ICs. If a control deficiency has been identified through the risk assessment process, this will be clear. If, however, the issue was identified through other sources such as the media or an audit, it may not be clear. Not all problems are control-related. There could be a significant exposure to risk and/or a potential for loss of significant financial resources that result from informed management decisions, not from a control deficiency. Management may determine to pursue a certain strategy or policy that is inherently risky. The mere exposure to risk does not automatically dictate that there is a control deficiency. For example, resource limitations may prevent an organization from achieving its mission, but unless it is the result of a control deficiency, it should not be included in the SOA. Issues must be control-related to be included in an MICP Certification Statement. Other issues should be addressed elsewhere (i.e., budget process, responses to audit recommendations, direct briefs to the Agency Director).

3.13.2. Does the issue meet any of the general criteria for materiality (Threat to Mission, Threat to Resources, or Threat to Image)?

3.13.2.1. Threat to Mission. Consider whether the control deficiency presents a risk to achieving the mission of DCMA. Threats to Mission include but are not limited to:

- 3.13.2.1.1. Impaired fulfillment of essential mission or operations.
- 3.13.2.1.2. Unreliable information causing unsound management decisions.
- 3.13.2.1.3. Violations of statutory or regulatory requirements.
- 3.13.2.1.4. Impact on information security.
- 3.13.2.1.5. Depriving the public of needed Government services.

3.13.2.2. Threat to Resources. Consider whether the control deficiency is a threat to physical, financial or human resources. Both actual loss and potential for loss of resources should be considered along with the magnitude and frequency of the loss. When a control deficiency has a clear dollar value associated with it, the general standard used for materiality is a one percent threshold. Anything greater than 1 percent of DCMA's budget would be considered material.

3.13.2.3. Threat to Image. Finally, consider the impact on the DCMA image. A control deficiency may not pose a threat to the mission or a material threat to resources, but it may bring substantial negative publicity. These control deficiencies could be material even if they do not meet the first two criteria. Threats to image include but are not limited to:

3.13.2.3.1. Sensitivity of the resources involved (e.g., drugs, munitions).

3.13.2.3.2. Current or probable congressional or media interest.

3.13.2.3.3. Diminished credibility or reputation of management.

3.13.3. Is the issue directly related to the DCMA mission?

3.13.3.1. Once an issue is determined to be control-related and meets at least one of the three general criteria above, the final question is whether the issue is directly related to the DCMA mission.

3.13.3.2. The Matrix of Materiality (Table 5) can be used to help AUMs evaluate these questions:

Table 5. Sample Matrix of Materiality
Determine Materiality

	Date	Issue	Summary of Issue	Control Related	Threat to Mission	Threat to Resources	Threat to Image	DCMA Mission	Comments	Decision	Initial Date for Targeted Review
1	1/2/2013	Time and Attendance Process	Employees inaccurately reported time and attendance to the wrong PLAS codes	Y	N	Y	N	N	Reporting inaccurate PLAS codes could impede the accuracy and timeliness of critical mission-related information	Reportable Condition	3/1/2014
2	1/20/2013	Certification and Accreditation of DCMA IT Systems	DCMA is required by law to certify 90 percent of DCMA IT systems. ICs were not in place to ensure that this requirement was met	Y	Y	N	N	Y	This is a threat to the mission because of the inability to comply with law. The lack of certification of IT systems could impede the accuracy and timeliness of critical mission-related information	Material Weakness	4/1/2014
3	5/1/2013	Government Travel Program	Audit found inappropriate expenditures by four individuals in the amount of \$300,000	Y	N	N	Y	N	Although the amount of money is not material (i.e., less than 1 percent), there is the potential for negative media publicity. Since this was not directly related to the DCMA mission this will be reported as a reportable condition other than a material weakness	Reportable Condition	7/1/2014

3.14. MICP REPORTING CATEGORIES.

3.14.1 The AUM will designate each operational IC deficiency into one of the following reporting categories:

3.14.1.1. Acquisition.

3.14.1.1.1. The guidance in USD(AT&L) Memorandum (Reference (h)) applies to all acquisitions, including major acquisitions and items designated as major systems, subject to the procedures of the Defense Acquisition Board, the Military Services Acquisition Review Councils, or the Selected Acquisition Reporting System. Reference (h) requires the use of an acquisition assessment template when conducting IC reviews and reporting of IC material weaknesses. The purpose of the acquisition template is to assist in the:

3.14.1.1.1.1. Determination of risks related to proper implementation.

3.14.1.1.1 2. Evaluation of existing controls and monitoring activities.

3.14.1.1.1 3. Consideration of corresponding standards and success factors.

3.14.1.1.1 4. Determination of new material weaknesses.

3.14.1.1.2. OMB Memorandum (Reference (i)) and DoDD 5000.01, “The Defense Acquisition System” (Reference (p)) may be helpful when evaluating a material weakness for inclusion in this category by providing a template that is organized by four interrelated cornerstones as a foundation for evaluating the acquisition function, and by providing acquisition policies that govern the Defense Acquisition System, respectively.

3.14.1.2. Communications. Communication requires a sender, a message, and an 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.

3.14.1.3. Comptroller and/or Resource Management. Comptroller and/or 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 DoD personnel and all financial management areas not covered by other reporting categories, including those in connection with OMB Circular A-123 (Reference (e)).

3.14.1.4. Contract Administration. Contract administration covers 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, in accordance with USD(AT&L) Memorandum (Reference (h)) and OMB Memorandum (Reference (i)).

3.14.1.5. Force Readiness. Force readiness includes the operational readiness capability of combat and combat support (both Active and Reserve) forces which provides the necessary flexibility to deter potential foes and rapidly respond to a broad spectrum of global threats.

3.14.1.6. 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, other intra-agency or intergovernmental agency resources or personnel.

3.14.1.7. Intelligence. Intelligence is 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.

3.14.1.8. Manufacturing, Maintenance, and Repair. Manufacturing, maintenance, and repair covers the management and operation of in-house and contractor-operated facilities performing maintenance and repair of and/or installation of modifications to materiel, equipment, and supplies. It also includes depot and arsenal-type facilities as well as intermediate and unit levels of military organizations.

3.14.1.9. Other. Other is all functional responsibilities not represented by any other functional category, including management and use of land, sea, and air transportation for movement of personnel, material, supplies, and equipment using military and civilian sources.

3.14.1.10. Personnel and Organizational Management. Personnel and organizational management covers authorizations, recruitment, training, assignment, use, development, and management of military and civilian DoD personnel. It also includes the operations of headquarters' organizations. Contract personnel are not covered by this category.

3.14.1.11. Procurement. Procurement covers 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).

3.14.1.12. Property Management. Property management covers construction, rehabilitation, modernization, expansion, improvement, management, and control over real property (both military and civil works construction), to include installed equipment, and personal property. It also covers disposal actions for all materiel, equipment, and supplies including the Defense Reutilization and Marketing System.

3.14.1.13. Research, Development, Test, and Evaluation. This covers the basic project definition, approval, and transition from basic research through development, test, and evaluation and all DoD and contractor operations involved in accomplishing the project work, excluding the support functions covered in separate reporting categories such as Procurement and Contract Administration.

3.14.1.14. Security. Security is the plans, operations, systems, and management activities for safeguarding classified resources (not peripheral assets and support functions covered by other reporting categories). It also covers the DoD programs for the protection of classified information.

3.14.1.15. Security Assistance. Security assistance is the management of DoD Foreign Military Sales, Grant Aid, and International Military Education and Training Programs.

3.14.1.16. Supply Operations. Supply operations encompasses 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). It 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).

3.14.1.17. Support Services. Support services includes all support service functions financed from appropriate funds not covered by the other reporting categories such as health care, veterinary care, and legal and public affairs services. All nonappropriated fund activities are also covered by this category.

3.14.2. When reporting financial reporting or financial system IC issues according to assessments, the AUM will classify the end-to-end business processes affected by the control issue. The following IC categories will be used to classify the control issue:

3.14.2.1. Budget-to-Report. 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.

3.14.2.2. Hire-to-Retire. Hire-to-Retire encompasses the business functions necessary to plan for, hire, develop, assign, sustain, and separate personnel in the AU.

3.14.2.3. Order-to-Cash. 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.

3.14.2.4. Procure-to-Pay. 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.

3.14.2.5. Acquire-to-Retire. 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.

3.14.2.6. Plan-to-Stock. 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.

APPENDIX A
SAMPLE STANDARD MEMO



DEFENSE CONTRACT MANAGEMENT AGENCY
3901 A AVENUE, BUILDING 10500
FORT LEE, VA 23801-1809

MEMORANDUM FOR AGENCY MICP COORDINATOR

Subject: MICP CERTIFICATION STATEMENT

Ref: DCMA-INST 710 Managers' Internal Control Program Policy

[Insert AUM] evaluated the system of internal controls (ICs) in effect during Fiscal Year **XXXX**, completing **[insert number]** of completed IC assessments. The evaluation was performed in accordance with the policies contained in reference.

Information to support the certification was derived from management reviews, audits, inspections, Sub-AU's MICP Certification Statements and other management information, including knowledge gained from daily operations of programs and functions. An overview of the evaluation and related accomplishments is attached at Tab A.

I have **[reasonable assurance or reasonable assurance with exceptions or no assurance]** that management controls are in place and operating effectively and that the objectives of the Federal Managers' Financial Integrity Act were achieved providing **[a qualified certification or an unqualified certification with the exception of the issues identified attached at Tab B-1, Tab B-2, and Tab B-3 or no assurance based on.....]**.

My point of contact is **[Insert AUA name]**. She/he may be reached at **[Insert AUA phone number and email address here]**. Prepared by: **Name, Code, Phone number of preparer**

Signed by AUM
(Signer can sign and date electronically)

Attachments links:

Tab A: Accomplishments link to 360 page

Tab B-1: Listing of Material Weaknesses, Reportable Conditions and Control Deficiencies; Uncorrected and Corrected link to 360 page

Tab B-2: Uncorrected Material Weaknesses, Reportable Conditions, and Control Deficiencies link to 360 page

Tab B-3: Corrected Material Weaknesses, Reportable Conditions, and Control Deficiencies link to 360 page

**APPENDIX B
SAMPLE (TAB A)
FY XXXX Accomplishments**

Date: **xx/xx/xxxx**

Created by: **Name of Person - AU-Sub AU**

Component with Primary Responsibility (CPR) AUM: **Name of Person – CPR AUM (Must match the Agency Process Inventory)**

Name of Problem/Project/Effort: **Self Explanatory**

Associated Program or Process: **Must match the Agency Process Inventory**

Functional Category: **See the Agency Process Inventory**

Line of Service: **See the Agency Process Inventory**

Description of Issue: **Problem**

Actions: **Action taken to resolve the problem**

Results: **Quantifiable evidence of the accomplishment including evidence of return on investment of actions made to accomplish the improvement**

Point of Contact: **Execution or CPR SME or team**

Approver: **AUM or Sub-AUM (Digital Signature Required)**

NOTE: Accomplishments MUST document Internal Control Improvements NOT Mission Requirement Activity. In other words, “doing your job” is not an accomplishment; articulating how you improved “doing your job” by improving internal controls IS an accomplishment.

**APPENDIX C
 SAMPLE (TAB B-1)
 List of all Uncorrected and Corrected
 Material Weaknesses - Reportable Conditions - Control Deficiencies**

Uncorrected Material Weaknesses - Reportable Conditions - Control Deficiencies					
Title	Issue Type	Year First Reported	Targeted Correction Date Reported in Last Statement	Targeted Correction Date This Statement	Page #
If new the title must be specific and unique to the problem documented	Material Weakness or Reportable Condition or Control Deficiency	FY XXXX	1 st 2 nd 3 rd 4 th QTR.FY XXXX	1 st 2 nd 3 rd 4 th QTR.FY XXXX	Page # reported in this document.

Corrected Material Weaknesses - Reportable Conditions - Control Deficiencies					
Title	Issue Type	Year First Reported	Targeted Correction Date Reported in Last Statement	Corrected Date	Page #
Title as reported in previous report	Material Weakness or Reportable Condition or Control Deficiency	FY XXXX	FY XXXX	1 st 2 nd 3 rd 4 th QTR.FY XXXX	Page # reported in this document.

NOTE: If a problem is discovered and corrected within the same reporting period, it is considered an accomplishment and will be reported in Appendix B (Tab A) of the Certification Document.

APPENDIX D
SAMPLE (Tab B-2)
Uncorrected Material Weaknesses - Reportable Conditions - Control Deficiencies

Uncorrected Material Weakness-Reportable Condition-Control Deficiency		
Date Identified	XX/XX/XXXX	
Issue Type	Material Weakness or Reportable Condition or Control Deficiency	
Title	Must match Tab B-1	
Associated Program or Process	Must match the Agency Process Inventory	
Functional Category	Must match the Agency Process Inventory	
Line of Service	Must match the Agency Process Inventory	
Created by		
	Name of the employee identifying the issue	
CPR SME		
	Subject Matter Expert as listed on the Agency Process Inventory	
Assessable Unit Manager		
	As listed on the Agency Process Inventory	
Year Identified		
	FY XXXX Must match Tab B-1	
Original Targeted Correction Date	1 st or 2 nd or 3 rd or 4 th QTR FY XXXX Must match Tab B-1	
Targeted Correction Date in Last Year's Report	1 st or 2 nd or 3 rd or 4 th QTR. FY XXXX Must match Tab B-1	
Current Target Correction Date	1 st or 2 nd or 3 rd or 4 th QTR FY XXXX Must match Tab B-1	
Reason for Change in Current Target Date	Document the reason for change in last year's target date. If date the did not change document "N/A."	
Description of Issue		
	Description of the Problem or Issue	
Significance of Issue		
	Documentation of the magnitude of resources (people, time, money) that are affected by this issue	
Source(s) Identifying Issue		
	Describe how issue was identified.	
Results Indicator		
	Define the measure used to ensure issue does not reoccur. (Document specific control identified to correct the issue, training initiated, template initiated, etc.)	
Validation Process		
	Define how the corrective action will be verified (assessment of process, survey, audit)	
Completed Milestones	QTR	Description of the Completed Action
	FY XXXX	
Planned Milestones	QTR	Description of the Proposed Action
	FY XXXX	

APPENDIX E
SAMPLE (Tab B-3)
Corrected Material Weaknesses - Reportable Conditions - Control Deficiencies

Uncorrected Material Weakness-Reportable Condition-Control Deficiency		
Date Identified	XX/XX/XXXX	
Issue Type	Material Weakness or Reportable Condition or Control Deficiency	
Title	Must match Tab B-1	
Associated Program or Process	Must match the Agency Process Inventory	
Functional Category	Must match the Agency Process Inventory	
Line of Service	Must match the Agency Process Inventory	
Created by		
	Name of the employee identifying the issue	
CPR SME		
	Subject Matter Expert as listed on the Agency Process Inventory	
Assessable Unit Manager		
	As listed on the Agency Process Inventory	
Year Identified		
	FY XXXX Must match Tab B-1	
Original Targeted Correction Date		
	1 st or 2 nd or 3 rd or 4 th QTR FY XXXX Must match Tab B-1	
Targeted Correction Date in Last Year's Report		
	1 st or 2 nd or 3 rd or 4 th QTR FY XXXX Must match Tab B-1	
Current Target Correction Date		
	1 st or 2 nd or 3 rd or 4 th QTR FY XXXX Must match Tab B-1	
Reason for Change in Current Target Date		
	If the current target changed from the last report to this report document reason for change. If date did not change document "N/A."	
Description of Issue		
	Description of the Problem or Issue	
Significance of Issue		
	Documentation of the magnitude of the resources (people, time, money) that are affected by this issue	
Source(s) Identifying Issue		
	Describe how the issue was identified.	
Results Indicator		
	Define the measure used to ensure the issue does not reoccur. (Document the specific control identified to correct the issue, training initiated, template initiated, etc.)	
Validation Process		
	Define how the corrective action will be verified (assessment of process, survey, audit)	
Completed Milestones		
	QTR FY XXXX	Description of the Completed Action

APPENDIX F
SAMPLE MICP Plan **MICP PLAN AU Name**
Manager's Internal Control Program (MICP) Plan

Fiscal Year (FY) associated with this plan: (Frequency should be at least annually.)

AUM: (Must match the Agency Process Inventory.)

AUA: (Must match the Agency Process Inventory.)

Overview of the MICP within AU: Address all five elements of the GAO standards (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring, and how they are being addressed within your organization.) For each discussion area, if published information already exists, it is unnecessary to repeat it within the document. Instead, attach or reference the location and source of the relevant information, so it can be easily obtained.

Control Environment

Mission. Document the AU mission.

Strategic Plan. Identify the AU strategic plan and identify how it aligns with the Agency strategic plan.

Organization Structure. Describe how the AU is structured—the hierarchy, functional divisions, programs, staffing, etc.

- Attach the dated organizational chart.
- Document how the key areas of authority and responsibility are defined. Identify how lines of reporting are established.

Risk Assessment. Describe how priorities are developed using assessment of risk (This section is a narrative overview of the risk assessment.)

Control Activities. Describe the methodology of how control activities are identified and developed, the types of policies and documented procedures that are in place to explain and outline how to ensure the effectiveness of the controls (DCMA-INST 501, "Policy Publications Program" requires that each instruction and annex indicate that the publication is subject to evaluation and testing in accordance with DCMA-INST 710, "Managers' Internal Control Program." It also identifies the location of process flowcharts that supplement narrative process descriptions unless the Policy Advisory Board has granted a waiver.

Information and Communication. Describe how ICs are communicated to SMEs required for execution and how changes in controls are disseminated. Include information on the significant channels of communication, such as; email, website, monthly reports, etc.; the typical subject matter; the target audience; and the frequency of the communication.

Monitoring. Describe methods of monitoring activities/IC assessment being performed by both internal and external entities. Include self-assessments, evaluations and risk assessments.

- List the total number of scheduled IC assessments for the upcoming FY.
- List the total number of completed IC assessments for the previous FY.

Accomplishments. Describe how management documents accomplishments. Include types of performance measures and indicators (i.e., specific metrics) established to measure progress in process management and accomplishment of objectives and goals.

Corrective Action Plans. Describe how the AU records improvement requirements and actions required to respond to issues.

MICP Training. Document training schedule for employees within the AU.

Reporting Requirements. Document or plan for process documentation and/or assessment.

GLOSSARY

DEFINITIONS

Acquisition. The conceptualization, initiation, design, development, test, contracting, production, deployment, logistics support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in or in support of military missions.

Assessable Unit (AU). A subdivision (organization, functional, programmatic or other) of the Agency's total MICP, as designated by the Director, which allows for adequate IC of the subdivision to include: analysis, documentation, identification, and insertion of controls associated with the specific subdivision in order to mitigate identified risk. Each AU is required to have an appointed and adequately trained AUM and AUA to lead and administer the subdivision's MICP for the Agency Director and MICP Coordinator. The AU may be further divided into Sub-AUs by the Assessable Unit Manager.

Assessable Unit Administrator (AUA). Coordinates the MICP for their AUM; communicates with Agency MICP Coordinator on policy; annually coordinates the AU Certification and quarterly updates for AUM approval.

Assessable Unit Manager (AUM). The head of the AU, responsible for the MICP requirements of the AU. Appoints and supervises the AUA in the conduct of the AU MICP effort. Appoints and supervises the Sub-AU. The AUM manager must be a government employee, to prevent inherently governmental functions from being performed by contracted employees.

Control Deficiency. Control deficiencies exist 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.

Corrective Action Plans (CAPs). A written document that spells out the specific steps necessary to resolve a control issue, including targeted milestones and completion dates. CAPs for operational assessment deficiencies are maintained with the MICP documentation. CAPs for financial reporting and financial systems material weaknesses are maintained in the FIAR Planning Tool.

Internal Control (IC). Systematic documented measures (such as reviews, checks and balances, methods and procedures) instituted by a CPR SME to (1) conduct its business in an orderly and efficient manner, (2) safeguard its assets and resources, (3) deter and detect errors, fraud, and theft, (4) ensure accuracy and completeness of its accounting data, (5) produce reliable and timely financial and management information, and (6) ensure adherence to its policies and plans.

IC Assessment. A documented evaluation on the effectiveness and adequacy of the IC framework to meet the mission objectives.

Integrated Financial Management System (IFMS). A unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel, process (manual and automated), procedures, controls, and data necessary to perform financial management functions, manage financial operations of the agency, and report on the agency's financial status to central agencies, congress, and the public.

Levels Of Assurance. Explicit finding provided by the AUM or agency director as to the status of ICs in a reported element. One of three findings must be reported in the AU certification and the agency SOA: unqualified, qualified or no assurance.

MICP Coordinator. Program Manager of the MICP administers the agency-wide program to include policy, tools and training; maintains agency AU inventory; supports AUM and AUA in the conduct of their efforts; coordinates with USD(C) and USD(AT&L) on policy and administrative matters; and annually prepares the agency SOA and quarterly updates for approval.

Material Weakness. A specific instance of a failure in a system of control or lack of control that would significantly impair fulfillment of the agency's mission, violate statutory or regulatory requirements or significantly weaken safeguards against waste, loss, unauthorized use or misappropriation of funds, property or other assets. The material weakness may present a major impact to the environment, safety, security, or readiness of the command. Material weaknesses must be reported in the Agency SOA to the SD. A financial reporting material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. For an IC deficiency to be considered a material weakness:

(1) It must involve a weakness in ICs (such as ICs are not in place, are not being used, or are inadequate), which:

- (a) Impairs or potentially impairs essential operations or mission;
- (b) Significantly weakens established safeguards against waste, fraud, abuse, and mismanagement of resources;
- (c) Demonstrates substantial noncompliance;
- (d) Threatens the image, reputation, or credibility of the organization;
- (e) Compromises or weakens information security; or
- (f) Is determined during an external inspection and upheld as a significant finding.

(2) It must warrant the attention of the next higher level either for awareness or action.

Materiality. (ICONO): The risk of error or inability to accomplish mission objectives. The level of materiality is based upon management's judgment.

(ICOFR & ICOFS): The risk of error or misstatement on the financial statements that could occur and would impact management's or user's decisions or conclusions based on such statements. Materiality shall be considered when determining the extent of testing or work required to assess IC over financial reporting as well as what deficiencies should be reported.

No Assurance SOA. One of the three explicit levels of assurance that a FMFIA ICONO, ICOFR, or ICOFS SOA must take. No assurance provides no reasonable assurance that ICs are

effective because few or no assessments were conducted, the noted material weakness(es) are pervasive across many key operations or the IFMS is substantially noncompliant with federal requirements.

Qualified SOA. One of the three explicit levels of assurance that a FMFIA ICONO, ICOFR, or ICOFS SOA must take. A qualified SOA provides reasonable assurance that ICs are effective with the exception of one or more material weakness(es) or the IFMS is not fully compliant with federal requirements reported. The SOA must cite the material weaknesses in internal management controls that preclude an unqualified statement.

Process. Sequence of interdependent and linked step-by-step activities or course of actions with definite start and end points that must be followed in the same order to correctly perform a task. These activities consume one or more resources (people, time, money) to convert inputs into outputs. These outputs then serve as inputs for the next stage until a known goal or end result is reached.

Reasonable Assurance. An informed judgment by management regarding the overall adequacy and effectiveness of IC based upon available information that the systems of ICs are operating as intended according to Reference (b).

Reportable Condition. A combination of control deficiencies, which in management's judgment, represents significant deficiencies in the design or operation of ICs that could adversely affect the AU's ability to meet its IC objectives. A reportable condition specifically related to financial reporting is a combination of control deficiencies, which adversely affects the AU's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles. The criteria for a reportable condition means that there is a more than remote likelihood that a misstatement of the financial statements that is more than inconsequential will not be prevented or detected.

Risk. The probable or potential adverse effects from inadequate ICs that may result in the loss of resources or cause an agency component to fail to accomplish mission objectives through fraud, error, or mismanagement. Risk is measured by the likelihood and the impact of the event having a negative effect. Examples of risk contributors include: complex transactions, pilferable items, and cross-functional processes.

Senior Assessment Team (SAT). A team of senior level executives that provides oversight of assessing and documenting the effectiveness of ICs for financial reporting and financial systems. The DCMA SAT is the RMP.

Senior Management Council. A committee or board of senior level executives that convene to advise the Director on IC matters related to operations, financial reporting, and financial systems, to include the identification of IC material weaknesses that merit reporting as material weaknesses.

Statement of Assurance (SOA). An annual statement in memorandum format that provides the Director's explicit level of assurance on whether ICs are effective. The SOA is based on self-

assessments conducted for mission-essential functions relative to risk and identifies any material weaknesses, reportable conditions, and/or control deficiencies found and reported in the AUM's certifications during the assessments. The SOA provides detail of corrective action or a plan with prescribed milestones to promptly correct any material weaknesses, reportable conditions, and/or control deficiencies reported. The AUM Certifications are submitted to each leader's next higher level of authority, to the Agency MICP Coordinator. It is then consolidated for submission to USD(C) via USD(AT&L) as the DCMA SOA..

Sub-AU. Sub component of the AU identified to better document process assessment or to better establish documentation of standard process for AU execution.

Sub-AUA. Coordinates the MICP for their Sub-AUM; communicates with AUA on policy; annually coordinates the Sub-AU Certification and quarterly updates for Sub-AUM approval.

Sub-AUM. The primary responsible manager of the Sub-AU as designated by the AUM.

System Nonconformance. Instances in which financial management systems do not substantially conform to financial system requirements constitute system nonconformance as defined in Reference (e). Financial management systems include financial and financially related (or mixed) systems.

Systemic Weakness. A specific instance of a failure in a system of control or lack of control that is pervasive within the Agency and materially affects ICs across organizational and program lines, usually affecting more than one AU.

Unified Set of Systems. Systems that are planned for and managed together, operated in an integrated fashion, and linked together electronically in an efficient and effective manner to provide agency-wide financial system support necessary to carry out the agency's mission and support the agency's financial management needs.

Unqualified SOA. One of the three explicit levels of assurance that a FMFIA ICONO, ICOFR or ICOFS SOA must take. An unqualified SOA provides reasonable assurance that ICs are effective with no material weakness(es) reported or that the IFMS is in conformance with federal requirements. Each unqualified statement should describe how the level of assurance is supported and how assessments were conducted.

GLOSSARY

ACRONYMS

AU	Assessable Unit
AUA	Assessable Unit Administrator
AUM	Assessable Unit Manager (Directorate Head)
CAP	Corrective Action Plan
CPR	Component with Primary Responsibility
DCMA-INST	DCMA Instruction
DoDD	DoD Directive
DoDI	DoD Instruction
FIAR	Financial Improvement and Audit Readiness
FMFIA	Federal Manager's Financial Integrity Act
FY	Fiscal Year
GAO	Government Accountability Office
IC	Internal Control
ICOFR	Internal Control Over Financial Reporting
ICOFS	Internal Control Over Financial Systems
ICONO	Internal Control Over Non-Financial Operations
IFMS	Integrated Financial Management System
IG	Inspector General
IPP	Individual Performance Plan
IRT	Initial Review Team
MICP	Managers' Internal Control Program
MRT	Mission Review Team
OMB	Office of Management and Budget
OP-MIC	Operational Panel – Managers' Internal Control
PLAS	Performance Labor Accounting System
QTR	quarter
RMP	Resource Management Panel
SAT	Senior Assessment Team
SD	Secretary of Defense
SME	subject matter expert
SOA	Statement of Assurance

Sub-AU	Subordinate Assessable Unit
Sub-AUA	Subordinate Assessable Unit Administrator
Sub-AUM	Subordinate Assessable Unit Manager
U.S.C.	United States Code
USD(C)	Under Secretary of Defense, Comptroller
USD(AT&L)	Under Secretary of Defense, Acquisition, Technology and Logistics