United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240

TAKE PRIDE IN AMERICA

December 10, 2010

FINANCIAL MANAGEMENT MEMORANDUM 2011-001 (VI.A)

To: Assistant Secretaries
Bureau and Office Directors
Bureau Assistant Directors for Administration
Chief Financial Officers
Internal Control Coordinators

From: for Don Geiger
Acting Director, Office of Financial Management (PFM)

Subject: Guidance for Fiscal Year 2011 Integrated Internal Control Program

This memorandum transmits the Department of the Interior's (DOI) guidance for the FY 2011 Integrated Internal Control Program. The guidance includes activities and timeframes necessary to comply with the Federal Managers' Financial Integrity Act (FMFIA) and Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Controls,* including Appendix A, *Internal Control over Financial Reporting.* Guidance related to the Department's Audit Follow-up Program and compliance with OMB Circular A-50 has been issued under separate cover (See FMM 2010-22).

An integrated, risk-based approach will be more efficient and contain less redundancy in business process assessments that, if properly performed, will satisfy a variety of the Department's review and reporting requirements. Bureaus and offices must assess risk in a consistent manner using the Integrated Risk Rating Tool (IRRT), considering inherent risk, control risk, and fraud risk. Internal control reviews will focus primarily where risk is high.

This year's program will focus on strategies and activities to ensure maximum efficiency and effectiveness of Interior's programs and make certain that the risk of fraud is minimized. Bureaus and offices must address Interior's core mission areas, core and support business service areas, and enterprise (technology) service domains (identified in the DOI Business Model), by doing the following:

- Operating efficiently – implementing streamlined processes to eliminate waste and reduce cost. Operational efficiency can be viewed as the ratio of resources expended by agencies to outputs.
- Operating effectively – achieving intended programmatic goals and objectives.
- Managing and protecting resources.
- Complying with laws and regulations.
- Sustaining effective controls over financial reporting.
- Using reliable program and financial information for day-to-day decision-making.

In addition, an extra focus will be placed on the Financial Assistance and Acquisition and Payables business processes. The FY2010 Agency Financial Report indicated audit findings in these areas. The Department will form multi-bureau/office workgroups to review current processes and develop process improvements that can be implemented across all bureaus/offices.

To continue implementing the integrated, risk-based internal control program, bureau senior management directs the planning, reviewing, and reporting for internal control over all programs and operations including financial reporting. Senior leadership coordinates among the various offices involved including programs, finance, budget, acquisition, and information technology to successfully meet the requirements for maintaining, testing, and reporting on internal controls. Bureaus are encouraged to leverage existing senior management teams to serve as Senior Management Council and Senior Assessment Teams for internal controls.

The attached *Integrated Internal Control Program FY 2011 Annual Guidance* provides instructions and direction to facilitate compliance with FMFIA and OMB A-123 and to ensure that the Secretary's Annual Assurance Statement is accurate and adequately supported. Attachments 1 and 17 are the Schedules of Key Actions that outline key actions and deadlines for those actions. The guidance requires that bureaus and offices do the following:

- Planning
  - Verify component inventories and assessable units.
  - Identify and verify risks.
  - Integrate and coordinate internal control review activities.
- Evaluating Entity-Level Controls
  - Document and assess bureau/office-wide design of controls (including controls relating to financial reporting and information technology).
- Evaluating Process-Level Controls
  - Document key processes and controls.
  - Update the annual, risk-based Internal Control Review Plan, with a 3-year cycle.
- Testing Operating/Transaction-Level Controls
  - Perform control assessments and internal control reviews (ICRs.)
  - Document operating effectiveness of controls.
- Concluding, Correcting, and Reporting
  - Conclude on control effectiveness, suitability of compensating controls and whether any control gap is a material weakness.
  - Prepare and track corrective action plans as necessary.
  - Prepare a Statement of Assurance on Internal Controls Over Financial Reporting.
  - Prepare an Annual FMFIA Assurance Statement.

The Office of Financial Management will work with the bureaus to apply the Guidance for the Internal Control Program. PFM will encourage consistency in approach to assessing risk and use of PFM's templates for risk management and assessment of internal control. PFM plans to hold a lessons learned discussion at the end of the FY 2011 cycle.

We look forward to your cooperation and assistance as we continue to fulfill the Department's Internal Control Program responsibilities this fiscal year. The guidance is Attachment A to this

memo. If you have questions or would like to discuss the requirements set forth in this memorandum, please contact Eric Eisenstein, Division Chief, Internal Control and Audit Follow-up, at eric_eisenstein@ios.doi.gov or (202) 208-3417.

Attachments: As Stated

cc: Finance Officers Partnership
Assistant Inspector General for Audits
Department Audit Liaison Officers (ALOs)

Attachment A

Department of the Interior
Internal Control Program
Fiscal Year 2011 Annual Guidance

Table of Contents

Section Page

Attachments:

OMB Circular A-123

OMB Circular A-123, Appendix A

List of Figures

I. The Internal Control Program

The Department's Integrated Internal Control Program comprises the plans, methods, and procedures used to support meeting the Department's missions, goals, and objectives, and it supports performance-based management. In addition to helping to fulfill the Department's mission functions, the Department's Integrated Internal Control Program contributes to complying with other legislative requirements such as the Government Performance Results Act (GPRA), the Chief Financial Officers Act (CFO Act), the Inspector General Act of 1978, as amended, the Federal Financial Management Improvement Act of 1996 (FFMIA), the Federal Information Security Management Act of 2002 (FISMA), the Improper Payments Information Act of 2002 (IPIA), the Single Audit Act, as amended, and the Clinger-Cohen Act of 1996.

In fiscal year (FY) 2011, the Department will continue to employ the Integrated Risk Management Framework. The Framework considers the Department-wide objectives and relevant sources of risk from internal management factors and external sources and establishes control structure to address those risks. The Integrated Risk Management Framework is modeled after the Government Accountability Office's (GAO) Risk Management Framework model. The Framework integrates the Department's Mission Areas and Outcome Goals, the Department's Strategic Plan, and the Department's Business Model.

Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control helps the Department's program managers achieve desired results through effective stewardship of public resources. The goals for the FY 2011 Internal Control Program continue to be the following:

- to ensure senior management oversight and coordination at the department and bureau level;
- to develop and implement the Department's Integrated Risk Management Framework;
- to provide senior management with risk assessments for significant Departmental components;
- to implement a risk-based and cost-benefit based approach;
- to improve consistency and comparability of bureau internal control programs by continuing to refine the internal controls guidance, and providing tools, templates, and training; and,
- to improve the Department's Integrated Internal Control Program maturity level.

For the Department to maintain an effective internal control program, management and staff must continue to have an understanding and commitment to controls. Although responsibility for controls lies with management, all employees have a role in the effective and efficient operation of controls established by management.

Management at all levels is responsible to reasonably assure the following:

- Programs achieve their intended results;
- The use of resources is consistent with agency mission;
- Programs and resources are protected from waste, fraud and abuse;
- Laws and regulations are followed; and,
- Reliable and timely information is obtained, maintained, reported, and used for decision-making.

A. Governance Structure

In accordance with the Office of Management and Budget (OMB) Circular A-123 Interior has established a governance structure consisting of 1) a Senior Management Council, and 2) a Senior Assessment Team.

The Senior Management Council:

- is performed by Interior's Principals Operating Group (POG), which also serves as the Internal Control and Audit Follow-up Council,
- is chaired by the Assistant Secretary - Policy, Management and Budget (PMB),
- is comprised of all Assistant Secretaries, the Solicitor, the Deputy Assistant Secretary for Budget and Business Management, the Chief Information Officer, the Senior Procurement Executive, and the Inspector General (ex officio),
- provides senior-level oversight of the Internal Control program, resolves issues related to the program, and decides reporting issues for the Department's Annual Financial Report, and,
- ensures the Department's commitment to an appropriate internal control environment.

The Senior Assessment Team:

- is performed by the DOI Deputies Operating Group (DOG),
- is chaired by the Assistant Secretary – PMB,
- is comprised of Deputy Assistant Secretaries and bureau Deputy Directors,
- is responsible for implementing OMB Circular A-123 and to ensure assessment objectives are clearly communicated throughout the agency, and,
- ensures assessments are planned, conducted, documented, and reported in a timely manner.

The Internal Control Workgroup is comprised of bureau internal control coordinators, bureau finance representatives, and representatives from the CIO's office and the Office of Acquisition and Property Management. The Group meets regularly to discuss the status of the assessments of internal controls over both programs and financial reporting and related issues.

To promote the Internal Control Program at the bureaus, bureau senior management leadership directs the planning, reviewing, and reporting for internal control over all programs and operations including financial reporting. Senior leadership coordinates among the various offices involved, including program offices, finance, budget, acquisition, and information technology, to successfully meet the requirements for maintaining, testing, and reporting on internal controls. Bureaus are encouraged to use existing senior management teams to serve as Senior Management Council and Senior Assessment Teams for internal controls. Senior management review of bureau key internal control functions should be documented.

B. Control Environment

In establishing the control environment, management must demonstrate its commitment to competence in the workplace. As bureaus and offices address the core mission areas relating to

resource protection, resource use, serving communities, and recreation, as well as the business service areas (e.g., revenue collection, grants) and enterprise/technology service domains of the Department's Business Model, management must clearly define areas of authority and responsibility, appropriately delegate the authority and responsibility throughout the agency, support human capital policies for hiring, training, evaluating and disciplining personnel, and uphold the need for personnel to have and maintain the correct knowledge and skills to perform their assigned duties. Also, the organizational culture of an entity should be defined by management's leadership in establishing standards for ethical behavior and tone within the organization that should flow to all levels of the control environment.

Management is responsible for developing and performing activities that align with the following elements of the Committee of Sponsoring Organizations (COSO) framework:

- **Control Environment –** The Control Environment sets the tone of an organization influencing the control consciousness of its employees.
- **Risk Assessment –** Risk Assessment is the identification and analysis of risks to achievement of program objectives, helping to determine how the risks should be managed.
- **Control Activities –** Control activities are the policies and procedures that help ensure that necessary actions are taken to address risks related to the achievement of the program's objectives.
- **Information and Communication –** Information and communication encompasses the activities required to identify and communicate information in a timeframe that enables employees to carry out their responsibilities and take actions.
- **Monitoring –** Monitoring is the process to assess the quality of the internal control system's performance over time, including regular management and supervisory activities.

II. The Internal Control Cycle

Internal control activities should be considered part of a continuing cycle of assessing the risks associated with each program component, identifying controls to mitigate that risk, and testing those controls to ensure they are working effectively. This section is exclusively dedicated to providing guidance for evaluating internal control over programs. For additional information on Interior's risk management approach and internal control review process, refer to the *Program Manager's Guide to Risk Management and Internal Control*. Internal control should be an integral part of the cycle that occurs each year for planning, budgeting, and managing. The following sections of the Guidance provide an overview of the Internal Control Program cycle for program managers.

A. Verify Internal Control Components
B. Identify and Verify Risks
C. Document Key Processes and Controls
D. Assess Internal Controls
E. Document Results and Implement Corrective Actions
F. Monitor Corrective Actions and Document Lessons Learned

Figure 1 on the following page illustrates this cycle.

Department of the Interior
Internal Control Program Cycle

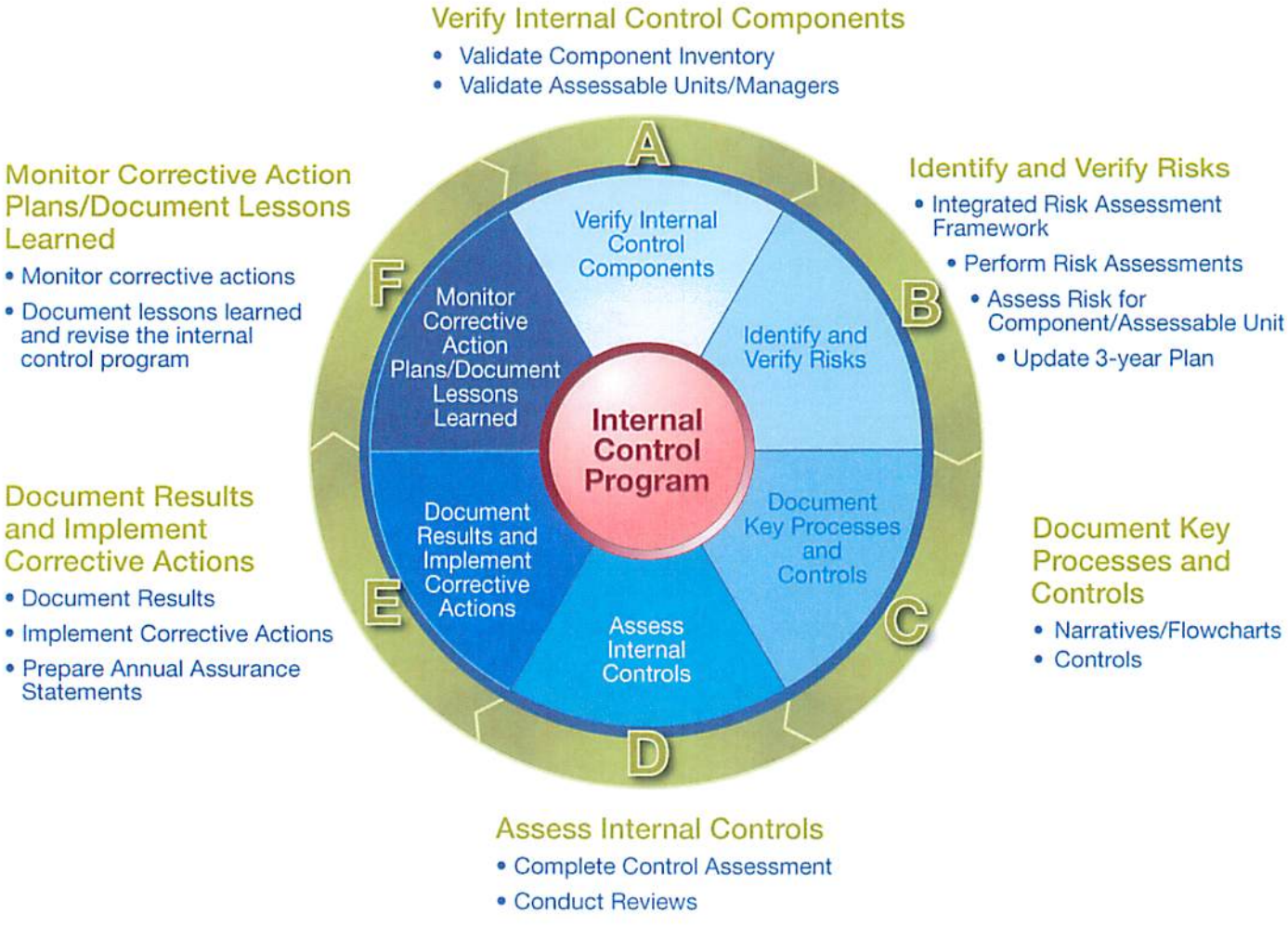

Figure 1: Internal Control Program Cycle

A. Verify Internal Control Components

This step includes: validating the component inventory; validating the assessable units and assessable unit managers; coordinating stakeholder communication; and identifying the review team.

1. Validate Component Inventory

Each bureau must validate, update, and submit a revised component inventory using the due dates contained in Attachment 1 (Note: Attachment 1 contains all deliverable due dates for the entire fiscal year.) It is important to review and validate existing components, identify new components, and refine the component structure to better support the bureau's mission or organization each year. This guidance requires bureaus to review and update their component inventory for the upcoming fiscal year using Attachment 2 (columns A through E).

A **component** is a bureau's significant programs, organizations, administrative activities, or functional subdivisions that flow from and are linked to the bureau's entity-wide objectives and strategic plans. A component has one or more sets of controls. Quantitative factors (those that have high dollar value) and qualitative factors (those that may be of particular interest to OMB, the public, or Congressional oversight committees, politically sensitive programs, or programs susceptible to fraud) should be considered to ensure that all of a bureau's significant programs are included. A **component inventory** is a list of all identified components. The component inventory should align with the bureau's mission and strategic plan. This can be accomplished by reviewing the bureau's organization chart as well as budget alignment, and structure used for Activity Based Costing (ABC). For example, FWS has the following components within their bureau:

- National Wildlife Refuge System
- Law Enforcement
- Business Management and Operations

2. Validate Assessable Units/Managers

Once a bureau component inventory has been identified, the sub-components, or assessable units, must be considered. An **assessable unit** is a subdivision of a component that is capable of being evaluated by risk and internal control assessments. Assessable units can be programs, program activities, or processes that are significant to a component's goals and objectives. Identification of components and subdivisions of components into assessable units ensures all significant processes within the bureau are identified and reviewed. An **assessable unit** should be large enough to allow managers to evaluate a significant portion of the activity being examined, but not so large that managers cannot perform a meaningful evaluation without extensive time and effort. Assessable units usually exist below the organizational chart level. Each **assessable unit** should have a unit manager who will be responsible for ensuring appropriate risk assessments and control testing are performed and documented. As with the component inventory, the inventory of assessable units must be validated each fiscal year and adjusted if necessary.

Continuing with the example given above, three components have been identified: National Wildlife Refuge System, Law Enforcement, Business Management and Operations. Within one component, National Wildlife Refuge System, the following assessable units exist:

- Wildlife Resources
- Division of Natural Resources
- Fire Management
- Division of Visitor Services and Communication

B. Identify and Verify Risks

1. Integrated Risk Management Framework

In FY 2009, the Department implemented an Integrated Risk Management Framework. The Integrated Risk Management Framework is modeled after the Government Accountability Office's Risk Management Framework model. The Framework integrates the Department's Mission Areas and Outcome Goals, the Department's Strategic Plan, and the Department's Business Model. As an example, **Figure 2** illustrates the Integrated Risk Management Framework for the Bureau of Reclamation's Hydro-Power Supply Management Function. The Framework considers Department-wide objectives and relevant sources of risk from internal management factors and external sources and establishes a control structure to address those risks. The Framework "integrates" the Internal Control Program Component Inventory and Assessable Units, Key Business Processes, Risk Assessments, and Control Assessments.

The Integrated Risk Management Framework is designed to improve consistency and comparability of each bureau's risk assessments. The Framework is intended to be flexible and scalable. The process for determining risk ratings high (red), medium (yellow), or low (green) is provided in the following section on *Performing Risk Assessments*.

The Framework will be used for identifying and addressing major performance and accountability challenges and high-risk areas. Some of the anticipated benefits of the Framework include:

- Gaining the opportunity to examine potential risks that may not be otherwise formally reviewed for certain programs (i.e., human capital, budget, etc.);
- Leveraging existing reviews and receiving formal acknowledgement of strong internal control practices;
- Gaining access to tools and templates that may not be currently used;
- Conveying knowledge to other organizations that are less developed in the risk assessment process (i.e. sharing best practices);
- Following a structured, disciplined approach and detailed guidance for conducting risk assessments;
- Gaining a comprehensive understanding of inherent risks in programs and the control activities in place to address these risks;
- Assessing and improving effectiveness of control activities and, therefore, program performance; and,
- Providing a process for managing risk when changes occur in the organization.

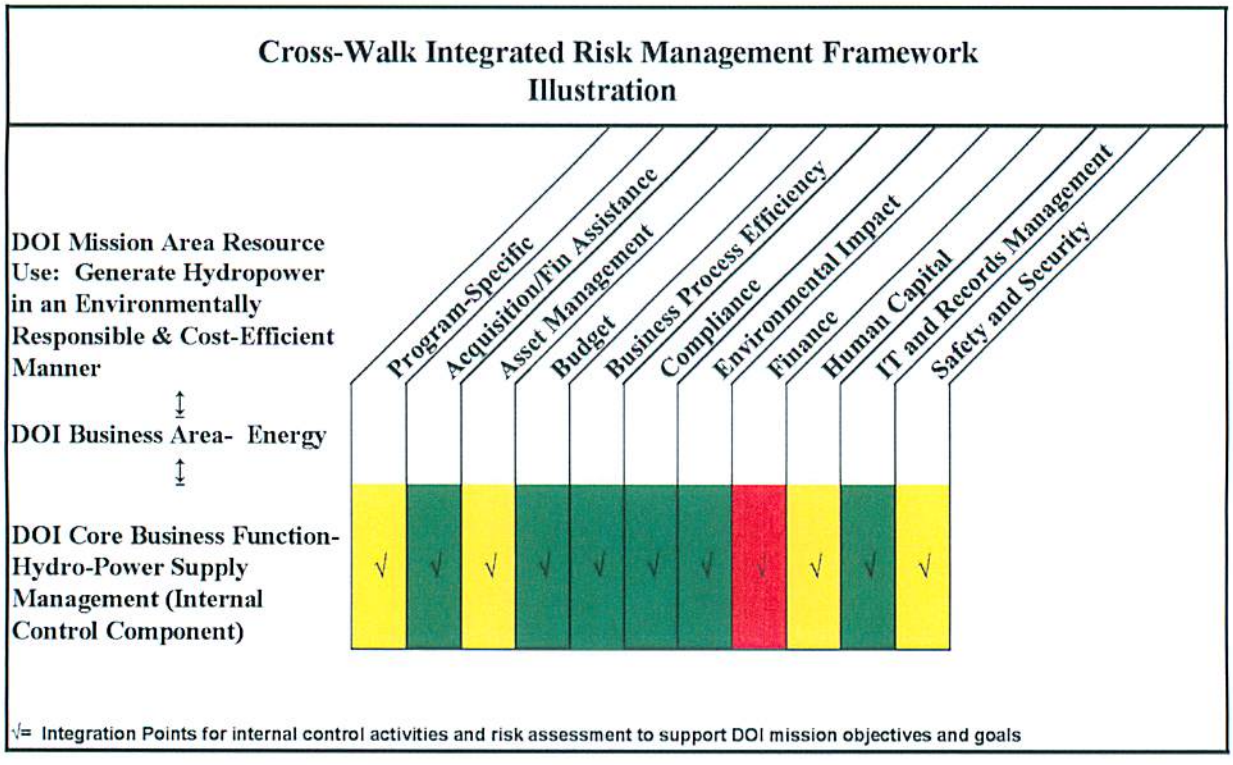

Figure 2: Integrated Risk Management Framework for the Bureau of Reclamation's Hydro-Power Supply Management Function

2. Perform Risk Assessments

Risk assessment is an internal management process conducted to ensure that an organization:

- Identifies, assesses, and considers the consequences of events that could prevent the achievement of its goals and objectives and/or could result in significant loss of resources;
- Identifies, analyzes, and manages risks relevant to achieving the objectives of safeguarding assets; and,
- Is in compliance with relevant laws and regulations.

Risk is the possibility that events could occur or might not occur and, as a consequence, result in adverse outcomes. Once the process and related components and assessable units are identified and related goals and objectives defined, management must identify the risks that could impede the efficient and effective achievement of those objectives. Risk challenges include traditional, irregular, catastrophic, and disruptive risk. Management should also consider conditions described in auditor-identified findings, noncompliance with laws and regulations, as well as issues found during internal control reviews. The types of risks to be considered include:

- **Inherent Risk –** includes conditions or events that exist which could negatively impact achieving the mission or objectives assuming no controls are in place. Also includes the nature of the program (component/assessable unit) and whether the program had significant

audit findings, or, the potential for waste, loss, unauthorized use, or misappropriation due solely to the nature of an activity itself.

- **Control Risk –** is the risk that controls may fail to prevent or detect identified inherent risks;
- **Residual Risk –** the risk that remains after management's response to risk (considering controls that are in place); and,
- **Fraud Risk –** the risk that there may be fraud or misuse of assets that causes appropriated funds to be wasted, preventing the program from achieving its mission. Fraud Risk should be considered for all risk categories.

To ensure an integrated approach, the Department's Integrated Risk Management Framework provides a list of risk categories and related risk factors that apply to most components/ assessable units (see Attachment 4). The list is a beginning point, and is not all-inclusive nor will every item apply to every agency or activity within the agency. Even though some functions and points are subjective in nature and require the use of judgment, they are important in performing a risk assessment. Management should consider these risk categories and factors, as applicable, when assessing risk for components/assessable units. There are three factors that determine the significance of the risks you have identified:

1. The consequence of the risk.
2. The likelihood of occurrence.
3. Management's capacity in acceptance of risk.

3. Assess Risk for Component/Assessable Unit

After management has identified existing risks, the risks must then be assessed as to their likelihood of occurrence and consequence of impact. **Likelihood** is the probability that the event could occur. **Consequence** is the impact of the event should it occur.

Risks must then be assessed as high, medium, or low. High risk areas could have a significant impact on the component or assessable unit's operations, efficiencies, or compliance; low risk areas would not materially impact operations, efficiencies, or compliance. High impact risk areas must be assessed to confirm effective mitigating internal controls are in place and operating as management intends. Risk assessment should be accomplished by a multi-disciplinary team.

Planning internal control reviews to be performed in the coming fiscal year should be a result of the risk assessment and control testing. The following figures can be used to determine the level of risk. **Figure 5** uses a scale of 1 to 5 for likelihood of occurrence and consequence of impact to determine high, medium, or low risk.

1. Insignificant	• No impact on the program • Very low impact on financial information
2. Minor	• Consequences can be absorbed under normal program operating conditions • Potential impact on the program • Low impact on financial information
3. Moderate	• There is some impact on the program objectives • Moderate impact on financial information
4. Major	• Severe injury • Significant property or resource damage • High level risk that impact ability to meet program objectives • Program goals or objectives are impacted • Major impact on financial reports
5. Catastrophic	• Failure to meet program objectives • Loss of life, immediate danger to health or property • Significant environmental/ecological damage • Significant financial loss

Figure 3: Consequence of Impact

1. Rare/Remote	Event may only occur in exceptional circumstances
2. Unlikely	Event could occur in rare circumstances
3. Possible	Event could occur at some time
4. Likely	Event will probably occur in most circumstances
5. Almost Certain	Event is expected to occur in most circumstances

Figure 4: Likelihood of Occurrence

Likelihood of Occurrence	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	Medium	High	High	High
Likely	Medium	Medium	Medium	High	High
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare/Remote	Low	Low	Low	Medium	Medium

Consequence of Impact

Figure 5: Depiction of the Risk Based on the Consequence of Impact *and the Likelihood of Occurrence (see Figures 3 and 4 for detail)*

The Department introduced the Integrated Risk Rating Tool (IRRT) to each bureau/office during FY 2009 as a consistent means of assessing risk throughout the Department. This tool is an automated way to assess risk described in this section. In FY 2011, all bureaus/offices are required to use the tool to assess risk for each assessable unit in the component inventory and to document the results on Attachment 3. The IRRT contains tabs for each risk factor noted in Attachment 4 and asks questions that will determine the likelihood of occurrence and the consequence of the potential impact to determine the inherent risk. After noting what controls are in place to mitigate those risks, a residual risk is then determined. Unless other arrangements are made with PFM, the bureaus/offices must use this tool, evaluate and summarize the results for each assessable unit, and transfer the risks onto the Risk Analysis page of Attachment 3. Transfer the resulting risk rating onto Attachment 2, Columns F through I.

It is important to note that risk assessments of information systems are prescribed by the National Institute of Standards and Technology (NIST) Special Publication (NIST SP) 800-30, *Risk Management Guide for Information Technology Systems*. The process for conducting a risk assessment stated in NIST SP 800-30 is similar to the process in A-123, enhancing the concept of integration.

4. Update the Risk-Based Internal Control Review Plan with a Three-Year Cycle

Validating each bureau's/office's annual comprehensive, risk-based internal control review plan under a three-year cycle is essential for effective implementation of A-123. After managers have assessed program vulnerabilities through risk assessment, they must develop a schedule for testing assessable units' controls which are used to mitigate those risks.

All assessable units with high inherent risk must be tested annually, if feasible. When all inherently high-risk assessable units are tested, managers will have documented support to enable them to accurately assess their controls. After a baseline has been established, and if there are no changes in key personnel, key systems, or key processes, rotational testing may be considered. If deficiencies are found, testing of that inherently high risk assessable unit should be conducted every year. The test schedule should be reflected on the three-year plan (Attachment 2, columns J through N). Some Information Technology (IT) controls must be tested annually as discussed in the FISMA.

Assessable units with medium risk ratings should be tested on a three-year cycle, while low risk assessable units should be incorporated into the testing schedule as resources permit but not less than once every five years.

Bureau personnel should look for opportunities to integrate, coordinate activities, and leverage internal reviews already being conducted elsewhere in the bureau. For instance, business processes and related IT systems that are key to each business process in accomplishing mission objectives must be assessed for effective internal control. FISMA requires comprehensive reviews of systems to ensure the effectiveness of information security controls that support operations and assets and certification and accreditation. OMB Circular A-123 requires testing of systems, including system security and restricted access, as well as FISMA- required testing of systems. Some of these requirements can be achieved in one assessment process. The Office of Acquisition and Property performs an entity-level review (*Conducting Acquisition Assessments under OMB Circular A123*, May, 2008) that provides support for the overall entity-level review being conducted by the Department. PFM, the OCIO and PAM are also focusing on a

coordinated, risk-based approach to assessing internal controls related to the IT and acquisition programs to determine which program-related areas are of the highest risk and should be assessed.

As another example, if the Office of Inspector General (OIG) is conducting an audit of a certain area of a program and is reviewing the internal controls within that area, it would be redundant for the assessable unit manager to implement an internal control review in that same area of the program.

Two types of control reviews are: Internal Control Review (ICR) and Alternative Internal Control Review (AICR). The difference between an ICR and an AICR is who conducts the review. A review conducted internally by the assessable unit manager is considered an ICR. A review conducted by other outside sources, (such as the OIG, GAO, or independent contractor), is considered an AICR.

Management may use other sources of information for planning purposes and to avoid duplication of conducting reviews. Sources of information may include the following:

- Management knowledge gained from daily operation of programs and systems (ICR),
- OIG and GAO reports, including audits, inspections, reviews, investigations, or other products (AICR),
- Annual evaluation and reports pursuant to FISMA and OMB Circular A-130, Management of Federal Information Resources, or any other system reviews (ICR).

However, the sources of information listed above should take into consideration whether the process included an evaluation of internal controls. Bureaus should avoid duplicating reviews which assess internal controls and should coordinate efforts with other evaluations to the greatest extent possible.

Departmental Functional Reviews (DFRs) – A DFR is a targeted review which is mandated by the Department and performed by the bureaus/offices which tests certain controls within a business process. To comply with statutory requirements, directives and risk-based analysis, the Department's Offices of the Chief Information Officer (OCIO), Acquisition and Facilities Management (PAM), and the Office of Occupational Health and Safety (OHS) may prescribe selected DFRs, for IT systems, property, financial assistance (i.e., grants and cooperative agreements), acquisition management, and other functional areas deemed necessary. These DFRs should be treated as a subset of an ICR. Guidance for conducting and reporting the results of these reviews will be provided by the responsible offices.

Use Attachment 2 to provide the updated component inventory/assessable unit inventory, the risk associated with each component and assessable unit, and an updated three-year plan. The schedule of key milestone dates (Attachment 1) has the due date for this submission. The three-year plan must identify test plan schedules for all components in a bureau's inventory regardless of when that component will be reviewed.

If bureaus need to defer, delay, or cancel any reviews from the priorities plan, they must justify in writing to the Office of Financial Management (PFM) the reason for these changes and explain how these changes do not weaken support for the assurance statement. **Requests must come from the Senior Executive Service (SES) official responsible for signing that component's assurance statement and be submitted to PFM as soon as the need is identified.**

It is important to note that, with the issuance of the American Recovery and Reinvestment Act of 2009 (ARRA), bureaus must take into account the increased risks associated with complying with ARRA and ensure that appropriate internal control reviews are planned and conducted so that controls are designed properly and operate effectively to mitigate those risks. These additional internal control reviews should be noted separately on the three-year plan as reviews being conducted for ARRA.

Due to PFM / File Description	Due Date	Attachment Number
Component Inventory of Assessable Units	Second Quarter	2

C. Document Key Processes and Controls

Once entity-level management has identified its high-risk areas, component and assessable unit managers must consider whether their processes are included within the entity-level high risk parameters. If so, assessable unit managers should then identify their key programs' objectives and processes, perform assessable unit-level risk assessments, and identify risk areas that align with the entity-level high risks (as noted in the previous section). **Key Processes** are those processes that are integral to the successful achievement of the program's mission, consist of an entire end-to-end process, and may be cross-cutting; that is, a key process may involve several assessable units when documenting the entire end-to-end process. Once management has decided that a key process requires review because it is aligned within a high risk area, management should plan for a review, document the process and controls, and conduct a control assessment. The control assessment is described further in the following section.

Prior to documenting narratives, flowcharts, and internal controls in a control matrix, it is often beneficial to document the goals of a program / assessable unit, and describe what risks management seeks to mitigate by examining the control activities. In other words, management should define why they want to examine a program / assessable unit and identify what controls are failing to help the organization meet it goals or objectives (see Attachment 8b for an example).

1. Develop Narratives / Flowcharts

Once key processes are identified, the program manager should describe, in narrative form, the steps that are taken to perform the particular process. This should include all applicable laws, regulations, and policies that determine how an assessable unit operates, as well as any automated systems involved in the process. Program processes are generally contained in bureau policy memoranda, handbooks, directives and standards, etc. Ideally, a program has a current manual or handbook for each assessable unit. A narrative example has been provided in Attachment 8b.

Steps for Preparing a Narrative

- See Attachment 8b as a guide that can be used in conjunction with a flowchart and control matrix.
- Identify the relevant laws, policies, procedures, and guidance that govern the process.

- Identify Interior's relevant core mission area - resource protection, resource use, serving communities, and recreation – or other business or IT service area.
- Define the beginning and the end of the process.
- Document the steps taken throughout the process including:
  - Individuals conducting the activity
  - Documents created/completed
  - Information Technology systems accessed/updated
  - Decision points
  - Potential internal controls (identified as controls in the assessment phase).
- Number the potential internal controls so that the activity can be traced from the narrative to the flowchart to the control matrix.

The narrative should describe important activities in as much detail as would be required for a person unfamiliar with the key business process to understand it. To the degree possible, the narrative should group and describe activities that follow a linear progression.

Flowcharts are a good way to assist the bureaus in analyzing a program process for risks and key controls. Flowcharts should identify each key control point that is mentioned in the business process narrative.

Flowchart Template Description

A flowchart is a graphical representation of the steps described in the narrative. Flowcharts are useful because they: (1) show relationships between steps that are not easily described in a written format, (2) highlight control activities, and (3) allow users to potentially identify redundant activities. Flowcharts are an efficient way to document the key internal control points in a business process.. The flowcharts provide an effective way to confirm the accuracy of the transaction cycle narrative with the process owners, and identify where disparate processes could be standardized. Use consistent numbering in the narrative, flowchart, and control matrix to aid the reader in connecting the documents. For example, a control numbered "COOP 8.3.2" in the narrative should be reflected with the same title in the flowchart and control matrix. A flowchart template is provided in Attachment 8d. Details on how to prepare a flowchart are provided below.

Flowchart Template Instructions

The Assessable Unit Manager is responsible for preparing or delegating responsibility for preparing the flowchart. In some assessable units, staff responsible for daily operations may be of assistance with flowchart preparation as they are typically familiar with the process and internal controls within the assessable unit.

While preparing the narrative should generally precede that of the flowchart, in some cases, a narrative may not exist or be finalized at the time of flowchart preparation. In instances where a narrative does not exist, the following steps should be followed to prepare the flowchart:

- Identify process owner(s), and collect information regarding the key business process, via interviews, prior to flowcharting;
- Define the beginning and end of the process; and
- Understand which organizations, in addition to the assessable unit, are involved in the key business process.

The flowchart should be completed early enough to allow sufficient time to complete remaining internal control review items such as the control matrix. Assessable Unit Managers should consider the time requirements for preparing flowcharts, if they did not already exist, when preparing their internal control review timelines.

Steps for Preparing to Draft a Flowchart

- Identify key individuals/groups within the process
- Define the beginning and the end of the process
- Document the steps taken throughout the process including:
  - Documents created/completed
  - Information Technology systems accessed/updated
  - Key decision points
- Identify controls within the process

Interior is making a concerted effort to demonstrate the successes of its programs, activities, and functions, toward its mission goals, through the Internal Control Program. Assessable Unit Managers should submit draft or final narratives to their bureaus' Internal Control Coordinator.

2. Controls

Controls are all the methods by which a component/assessable unit governs its activities to accomplish its mission. Simply put, controls are all the things a program does to ensure what is supposed to happen does happen, and what should not happen does not. These include policies, procedures, and mechanisms in place to mitigate risk so that the program's mission can be realized. The quality of the controls is more important than the number of controls.

Control Activities help ensure management directives are carried out. Examples include: documentation (written procedure for handling receipt of incorrect shipments of supplies), segregation of duties (using different personnel to purchase and receive goods), recording (comparison of inventory against inventory log), security (safes or locks), approvals, and authorizations. Controls over information systems also need to be in place. During times of change, controls must adjust to remain effective.

Key Controls are those critical controls which, if not executed, put the program objective at risk of failing. Key controls should be those controls that reduce risk to a low rating. Management relies upon these key controls to provide reasonable assurance of effective and efficient operations and compliance with applicable laws and regulations. An example is provided in Attachment 8e. Identify key controls in the Control Assessment Form tab of Attachment 3.

D. Assess Internal Controls

1. Complete Control Assessment

When assessing key controls, management should plan the assessment, and then determine if the control is designed properly before testing is conducted to determine if a control is working properly. Management should prepare a test plan (Control Assessment Form tab within Attachment 3) to test only the key controls for each process. For key controls that were designed

inappropriately, assumed ineffective, or that are non-existent resulting in high residual risk, bureaus should develop and implement mitigating corrective action plans to remediate the control weakness. For example, if an assessable unit does not have a policies and procedures manual outlining how the unit should operate, testing becomes a moot point. A corrective action plan should be put in place immediately to ensure that a policies and procedures manual is written and utilized.

2. Conduct Reviews

Controls in place that are designed properly, and that management believes to be effective, must be tested and documented to support management's assertions. Test methods include interviews, document analysis, observation, physical examination, questionnaires, and transaction testing. More than one method can be used when testing key controls.

Conducting the control assessment and planning the control testing should be documented using the Control Assessment Form and the Test Plan form in Attachment 3.

E. Document Results and Implement Corrective Actions

1. Document Results

Management must evaluate the results of control testing, using the Control Assessment form in Attachment 3, and document planned corrective actions using the Template for Corrective Action Plans in attachment 5. As a result of the assessment of key controls, management will conclude whether:

- There are control gaps; or,
- The operating effectiveness of the control is effective, partially effective, or not effective.

The results of testing will identify when a deficiency exists. The bureaus need to apply judgment to decide whether the consequences of ineffective controls are significant enough to report as material weaknesses. Internal control reporting efforts are subject to cost-benefit constraints, and no system is designed to provide absolute assurance that undesirable conditions will not occur. Bureaus must document the testing of internal controls and maintain documentation of the review for possible review by PFM and the OIG, as well as by bureau staff in a subsequent year.

A **control deficiency** exists when the testing of a control has failed. A control deficiency identified by the bureau should be reported to the next level of management; this allows the chain of command structure to determine the relative importance of each deficiency. A **significant deficiency (previously known as a reportable condition)** is a control deficiency, or combination of control deficiencies, that in management's judgment, should be communicated because they represent significant weaknesses in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives. A **material weakness** is significant deficiencies in which the agency head determines to be significant enough to report outside of the agency. Material weaknesses are communicated by the bureau in their annual FMFIA assurance statement and reported by the Department in the Annual Financial Report (AFR).

Determining the level of deficiency requires judgment by bureau managers as to the relative risk and significance of the deficiency. Component materiality should be considered in distinguishing material weaknesses from significant deficiencies and other deficiencies. A component that has a control deficiency or significant deficiency might rise to the level of material weakness if the component is material to the bureau/office's budget.

It is important to note that OMB guidance on reporting deficiencies for Information Technology systems is prescribed by FISMA and the definitions differ from those in A-123 and A-123, Appendix A. FISMA requires bureaus and agencies to report a significant deficiency as: "1) a material weakness under FMFIA, and 2) an instance of a lack of substantial compliance under FFMIA, if related to financial management systems. In this case, significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

Bureaus must notify PFM of material internal control weaknesses or noncompliance in a timely manner. A Corrective Action Plan (CAP) that addresses the weakness must be developed and submitted to PFM monthly for tracking purposes as discussed further below.

Due to PFM / File Description	Due Date	Attachment Number
Selection of Risk Analysis, Control Assessment, and Test Plan (all tabs)	09/15/11	3

2. Implement Corrective Actions

As stated above, the assessments of internal controls within key processes may identify weaknesses or deficiencies in internal control. To correct a deficiency, the assessable unit manager, together with Senior Management, should create a CAP. A CAP will most likely consist of revising or enhancing an already-existing control, or implementing a new control. A template for the CAP is included in Attachment 5.

CAPs should address the resolution of a specific identified control deficiency and include the steps and associated timelines required to complete the corrective action. An entry of "TBD" is not an acceptable target date for a corrective action plan. When developing a CAP to resolve any deficiency, use the standard CAP template and:

- State the as-is deficiency condition in the *Description of Finding / Recommendation* column. The deficiency should be briefly detailed and clearly stated.
- List the tasks to be accomplished to correct the deficiency in the *Corrective Action Tasks* column. Tasks should clearly describe what needs to be done in that step and should include a date the bureau/office/component expects to complete the task. It is recommended that the steps be a short duration from each other.

If system development and deployment is a bureau/office/component's solution to correcting a deficiency, the corrective action plan must include the following:

- A schedule for development and fielding to the point where the component believes the deficiency will be corrected, and internal controls will be effective;
- Tasks within the schedule demonstrating attention to internal controls which include addressing the five financial management assertions and the four system control assertions discussed in the Appendix A portion of this guidance; and
- Compliance with the Department Business Enterprise Architecture.

Deficiencies that slip year after year and do not meet target correction dates reflect negatively on the Department's commitment to improve. Therefore, the bureau's Senior Assessment Team should resolve deficiencies identified as material weaknesses and noncompliance issues as quickly as possible and ensure that the targeted correction dates are met. CAPs for material weakness and noncompliance issues must be provided to PFM with the related assurance statements.

Due to PFM / File Description	Due Date	Attachment Number
Template for Material Weakness/Noncompliance Corrective Action Plans	09/15/10	5

3. Prepare Annual Assurance Statements

The Department uses an integrated organizational structure to implement its internal control program. To ensure support for the Secretary's annual assurance statement, the chain of accountability begins with program managers, ascends to bureau and office directors, then to program assistant secretaries, and ultimately to the Secretary. Bureau and office directors should provide assurance statements to their assistant secretaries. **Bureaus and offices are required to obtain assurances from SES managers one level below the Deputy Director. Bureau and office Chief Information Officers must submit a separate assurance statement (template prescribed in the OCIO's guidance) to their director and provide a copy to PFM and the OCIO.**

Bureaus and offices are required to prepare an annual assurance statement that includes the following:

- Management's assertion about the effectiveness of internal control over operations, financial reporting and compliance with laws and regulations. All reviews, evaluations, and audits should be coordinated and evaluated to support the assurance.
- Assurance for Section 2, evaluating and reporting on the controls that protect the integrity of Federal programs, should be based on the results of internal control assessments that were completed in the current fiscal year.
- Assurance for Section 4 of FMFIA concerns the evaluation and reporting on financial systems that protect the integrity of Federal programs.
- Assurance for internal controls over financial reporting and any related material weakness and corrective actions must be identified separately.

Assurance should consider any FFMIA material weakness and non-compliance issues identified to date by financial statement audits for bureaus and offices. Bureaus and offices are required to

provide reasonable assurance as to substantial compliance with FFMIA and to identify any non-compliance in the three components of the FFMIA: financial system requirements, Federal accounting standards, and the U.S. Standard General Ledger at the transaction level. Also, a statement must be included regarding the bureau or office's general compliance with the FISMA requirements and Appendix III of OMB Circular A-130, Management of Federal Information Resources.

Bureau and office directors are required to submit their annual assurance statements through their assistant secretaries, and should ensure adequate time for assistant secretary review and approval so that each signed statement can be delivered on or before the date on which it is due. Templates that must be used for the September 30 annual assurance statements are provided in Attachments 6 and 7. Attachments to the assurance statement must include the following: summary of internal control reviews and results (as outlined in Attachments 6 and 7), material line items assigned to the bureau, and corrective action plans for any material weakness or noncompliance findings.

Due to PFM / File Description	Due Date	Attachment Number
FMFIA Assurance Statement	09/30/10	6 or 7

F. Monitor Corrective Actions and Document Lessons Learned

Monitoring the effectiveness of internal control should be incorporated into the normal course of business. Periodic assessments should be integrated as part of management's continuous monitoring of internal control and be reflected on the three-year control test schedule. Results of testing must be documented and corrections to deficiencies found as a result of an internal control review must be tracked by the bureau until implemented.

Summary reports on the results of the testing (i.e. a completed Attachment 3) from internal control reviews must be sent electronically to PFM; however, documentation to support the review should be maintained in the bureau/office. Documentation must comply with current OMB, GAO, and Department standards and should be accessible so that PFM and the OIG can perform compliance reviews. Status of corrective actions for any FMFIA material weaknesses identified by the bureau must be reported to PFM on a monthly basis.

Site Visits

PFM will conduct comprehensive site visits with each bureau to review progress in implementing ICRs and AICRs; to provide oversight and coordination in the assessment of internal controls; to review the adequacy and validity of assessable unit identification and risk assessments; to assess the documentation and testing of key controls over financial reporting; and the implementation of corrective actions to close out open audit recommendations.

Example

An example of the process or documenting the business process, developing a flow chart, and evaluating, testing, and documenting programmatic controls using the Department's Attachment 3 has been provided (Attachments 8a-e) as a reference.

***

The table below summarizes the instruction in Section II of this guidance and lists the key steps required to complete program reviews:

Action	Relevant Attachment	Due Date
Identify risk categories and related risk factors by using the List of Inherent Risk Factors.	4	--
Update the "Risk Analysis Form" of the Template for Risk Analysis, Control Assessment, and Test Plan.	3	Second Quarter
Update the Three-Year Component Inventory and Internal Control Review Plan and submit attachment.	2	Second Quarter
Identify key controls in the "Control Assessment Form" tab of the Template for Risk Analysis, Control Assessment, and Test Plan.	3	Second Quarter
Prepare test plans, identify key controls, and document test results in the "Control Assessment Form" and the "Test Plan Form" tabs of the Template for Risk Analysis, Control Assessment, and Test Plan.	3	Third Quarter
Document control assessment results in the Template for Risk Analysis, Control Assessment, and Test Plan for each review conducted and submit PFM-identified samples.	3	09/15/11
Document corrective actions for any identified material weaknesses or noncompliance issues in the Template for Corrective Action and submit the attachment.	5	09/15/11
Provide the Assurance Statement (attachment 6 or 7)	6 or 7	09/30/11

III. Appendix A, Assessment of Internal Control over Financial Reporting

FMFIA and OMB Circular A-123 apply to each of the three objectives of internal control: effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. While the standards of internal control are applied consistently toward each of the objectives, Appendix A requires the Department to specifically document the process and methodology for applying the standards when assessing internal control over financial reporting. Appendix A also requires management to use a separate materiality level when assessing internal control over financial reporting. The Secretary's annual assurance statement on the effectiveness of internal control over financial reporting required by Appendix A is a subset of the assurance statement required under FMFIA on the overall internal control of the agency.

Interior uses a top-down approach focusing on the assurance at the Department-wide level. This approach begins with the Department's significant consolidated financial reports and works back to material line items, bureau/offices business processes, process documentation and key controls.

This approach also focuses resources on the items most material and most at risk to Department's financial reporting.

Section 2 of the Department's Internal Control and Audit Follow-up Handbook provides guidelines to evaluate the internal controls over financial reporting. In addition, Attachments 9 - 19 to this Guidance provide templates and schedules for the FY2011 Appendix A effort.

IV. Appendix B, Improving the Management of Government Charge Card Programs

In August 2005, OMB issued Appendix B to OMB Circular A-123. This appendix requires agencies to maintain internal controls in government charge card programs. A significant requirement of this appendix is that agencies perform credit checks on all new purchase and travel card applicants. Each agency is required to maintain a charge card management plan. The required elements of the Department's charge card management plan are listed in Appendix B, but a significant requirement concerns performing credit checks on all new purchase and travel card applicants. The Office of Acquisition and Property Management (PAM) has issued a charge card management plan and it is located on its web site (www.doi.gov/pam) for reference.

This establishment and testing of internal controls is dictated in the management plan and each bureau procurement office is responsible for maintaining and testing internal controls in this area. The testing of other charge card-related controls should be performed where the controls are applied.

V. Appendix C, Requirements for Effective Measurement and Remediation of Improper Payments

Appendix C aims to improve the integrity of the government's payments and the efficiency of its programs and activities. On July 22nd, 2010 the President signed the Improper Payments Elimination and Recovery Act (IPERA) of 2010 into law. IPERA amends the Improper Payments Information Act (IPIA) of 2002 and repeals the Recovery Auditing Act (Section 831 of the FY 2002 Defense Authorization Act). IPERA expands the requirements of all agencies to periodically perform risk assessments of its programs and activities and identify those programs and activities that are susceptible to significant improper payments. Significant improper payments are defined by OMB Circular A-123 Appendix C as improper payments exceeding both 2.5% of annual program or activity payments and $10 million.

OMB Memo M-11-04, *Increasing Efforts to Recapture Improper Payments by Intensifying and Expanding Payment Recapture Audits*, was issued in November 2010 to address the recapturing of improper payments. OMB plans to issue final guidance on agency payment recapture audit programs, as required by IPERA, in January 2011. Until the issuance of the final guidance, bureaus/offices should follow OMB Memo M-11-01 and the existing guidance in OMB Circular A-123, Appendix C. The Department may issue further guidance when the final OMB guidance is issued.