September 19, 2006

FISMA FRAMEWORK

Introduction

The Federal Information Security Management Act (FISMA) requires that each agency perform an annual, independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. The Information Technology Committee of the Federal Audit Executive Council (FAEC) has been working on a project to enhance the consistency, comparability and completeness of evaluations performed in response to the requirements of FISMA. The resulting product is a framework for performing the FISMA evaluations. The framework provides an opportunity for the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) to endorse an approach designed to assist the Office of Inspector General (OIG) community with: (1) determining the current status of agency security programs through the testing of management and technical controls; (2) assessing management, policies, and guidances; and (3) providing feedback to agency management through the annual evaluation process that will better assist with establishing and achieving improvement goals for information security. The framework is based on Federal information security standards and guidelines developed by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB). While this framework parallels the Information Technology (IT) security self-assessment and other guidance used by Federal entities to internally assess their security program, the tests and procedures performed by the Inspectors General (IG) should ensure that an independent evaluation is performed as required by FISMA.

The Committee recognizes that a key to successful evaluations of information security programs is professional judgment. The Federal entities subject to FISMA requirements vary widely in size and complexity. Therefore, each OIG must independently decide upon the best approach. The intent of this framework is neither to promulgate standards nor otherwise commit IGs to performing or not performing certain security-related work. Rather, it is intended as a proactive measure that IGs can consider in completing the FISMA evaluations.

It is expected that a commonly accepted framework for the annual FISMA mandated reviews will help ensure the consistency and usefulness of the evaluations conducted by the OIG's. The framework supports the need for a risk-based approach with annual evaluations. However, it does not prescribe the specific elements of an information security program which need to be evaluated.

Key criteria supporting the framework are constantly changing and, in some cases, have not yet been finalized, which could impact implementation of a common framework. As we go forward, the FISMA framework needs to be carefully considered within the OIG community. There are several components within PCIE and ECIE that have a direct interest in this project, including the Audit Committee, the Inspection and Evaluation Committee, and the Information Technology Roundtable.

Framework

The FISMA framework considers and provides clarity on the following specific aspects related to FISMA requirements

1. Agency Security Programs

   An effective agency-wide information security program for purposes of the independent evaluation is defined by the requirements established in statute and guidance issued by the OMB and NIST, as implemented through the policies and procedures of each Federal entity. It is recognized in the Federal Information Security Management Act of 2002 that these may constitute minimum security requirements.

   There is considerable information available within both the public and private sector about controls that can be considered part of an information security program. Basic program controls may include: policy, planning, organization, technical, and performance analysis. Additionally, many Federal entities have unique security requirements that must be met due to their mission and the sensitivity of the information used to accomplish that mission. To achieve the goals of consistency of approach and comparability of results, the baseline for an evaluation of an information security program should make use of the controls indicated above. In essence, the cognizant IG will evaluate the adequacy of the security program as it relates to Federal government-wide requirements and implemented by the Federal entities under their respective cognizance.

2. Independent Evaluations

   The purpose of the independent FISMA evaluation is to determine with reasonable, but not absolute assurance, whether the confidentiality, integrity and availability of information are safeguarded by an agency-wide information security program comprised of program, management, technical and operational controls. According to FISMA, OIGs can determine the type of independent review: i.e., assessment, evaluation, or audit. Regardless of the type of the review conducted, there must be sufficient evidence on which to base a conclusion.

   OIGs will perform tests as part of required independent FISMA evaluations of a representative subset of information systems. The reviews will include coverage of the management, technical and operational controls identified by NIST in the *Federal Information Processing Standard (FIPS) 200* for protection of the confidentiality, integrity and availability of information and systems. The evaluation will also include program controls identified in numerous NIST publications for the overall information about a security program. The NIST guidance should be used by Federal entities in performing self-assessments which, in turn, the OIGs can review as part of their evaluations. Testing of financial applications and related general support systems as part of a financial statement audit performed in accordance with *Government Auditing Standards* and the *Federal Information System Controls Audit Manual* can be considered part of the testing of a representative subset of systems. Additionally, IT security reviews conducted during the year can serve as the source for an overall FISMA summary report. The use of FIPS 200 as the criteria for tests performed by the OIG will help ensure consistency, comparability and completeness of results from

annual FISMA evaluations. Also, FIPS 200 is fully supported by the upcoming issuance of NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

3. Professional Standards

All work performed by OIGs to comply with FISMA will comply with appropriate professional standards.

Each OIG should decide upon the professional standards, which should be used for completing the FISMA evaluation and how those standards should be implemented. The *Quality Standards for Inspectors General, Quality Standards for Inspections* and *Government Auditing Standards* may be used individually or as otherwise deemed appropriate.

4. Scope of Review

In accordance with FISMA, agency-wide information security programs include information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor or other source.

It is important to ensure that the OIGs' reviews of information security programs include support provided by other agencies and contractors. Coordination among Inspectors General is critical to ensure the efficiency and effectiveness of coverage provided to the information security programs of contractors.

The FISMA framework can support the use of a risk-based multi-year strategy for review of the security programs and systems of Federal entities. In that regard, it is contemplated that each OIG will exercise judgment, based on risk and other factors, in deciding which controls will be tested and how those tests will be performed.

5. Review Tools

The Information Technology Committee of the FAEC found that at least two sets of tools for review of information security programs are compatible with the proposed NIST framework and should be considered by OIGs for performing FISMA evaluations: (1) the information security baseline recommended by Control Objectives for Information and related Technology (CoBIT) and developed by the Information Technology Governance Institute; and (2) the maturity model contained in the Program Review for Information Security Management Assistance (PRISMA). (Note: The security guidance that formed the basis for PRISMA evaluations and maturity models is in the process of being replaced by the draft NIST SP 800-100, *Information Security Handbook: A Guide for Managers*. These tools can be used to help review the controls detailed in the NIST guidances. Also included is the list of NIST control areas and families.

FISMA Framework

I. Summary

For purposes of creating a FISMA evaluation framework, it was concluded that controls at both the program and system level can be evaluated to reach conclusions with regard to the adequacy of an information security program. The FISMA framework consists of the following control areas, which can all be traced directly to NIST guidance. Program controls are based on the draft NIST Special Publication 800-100, whereas the systems controls are from NIST Special Publication 800-53.

CONTROL AREAS

- **Program Controls**
- **System Controls**
  - **Management Controls**
  - **Technical Controls**
  - **Operational Controls**

NIST Draft SP 800-80, *Guide for Developing Performance Metrics for Information Security* states, "Each agency's information security program provides direct support to the agency mission. Information security performance metrics provide a means for the monitoring and reporting of agency implementation of security controls. They also help assess the effectiveness of these controls in appropriately protecting agency information resources in support of the agency's mission."

Each OIG must individually decide how risk assessments and evaluation tests and procedures are structured to analyze individual control areas and/or the overall security program.

II. Control Families

Each control area can be further defined by control families drawn directly from NIST Federal Information Processing Standard 200.

Control Areas	Control Families
Management	Risk Assessment
	Planning
	System and Services Acquisition
	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
	Physical & Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance
	System and Information Integrity
	Media Protection
	Incident Response
	Awareness and Training
Technical	Identification and Authentications
	Access Control
	Audit and Accountability
	System & Communications Protection

III. Program Level Control Evaluation

The following chart shows how program controls included in the FISMA framework can be further defined for purposes of designing and performing evaluation tests and procedures.

NIST Draft Special Publication 800-100 Program Controls		
Control Family	**Number**	**Name**
Information Security Governance	2.1	Information Security Governance Requirements
	2.2	Information Security Governance Components
	2.3	Information Security Governance Challenges and Keys to Success
System Development Life Cycle	3.1	Initiation Phase
	3.2	Development /Acquisition Phase
	3.3	Implementation Phase
	3.4	Operations /Maintenance Phase
	3.5	Disposal Phase
	3.6	Security Activities Within the SDLC
Awareness and Training	4.1	Awareness and Training Policy
	4.2	Components: Awareness, Training, Education, and Certification
	4.3	Designing, Developing, and Implementing an Awareness and Training Program
	4.4	Post-Implementation
	4.5	Managing Change
	4.6	Program Success Indicators
Capital Planning	5.1	Legislative Overview
	5.2	Capital Planning Roles and Responsibilities
	5.3	Identify Baseline
	5.4	Identify Prioritization Criteria
	5.5	Conduct System- and Enterprise-Level Prioritization
	5.6	Develop Supporting Materials
	5.7	IRB and Portfolio Management
	5.8	Exhibits 53 and 300 and Program Management
Interconnecting Systems	6.1	Managing System Interconnections
	6.2	Life-Cycle Management Approach
	6.3	Terminating Interconnection
Performance Measures	7.1	Metric Types
	7.2	Metrics Development and Implementation Approach
	7.3	Metrics Development Process
	7.4	Metrics Program Implementation
Security Planning	8.1	Major Applications, General Support Systems, and

NIST Draft Special Publication 800-100 Program Controls		
Control Family	**Number**	**Name**
		Minor Applications
	8.2	Security Planning Roles and Responsibilities
	8.3	Rules of Behavior
	8.4	System Security Plan Approval
	8.5	Security Control Selection
	8.6	Completion and Approval Dates
	8.7	Ongoing System Security Plan Maintenance
Information Technology Contingency Planning	9.1	Step 1: Develop Contingency Planning Policy Statement
	9.2	Step 2: Conduct Business Impact Analysis
	9.3	Step 3: Identify Preventive Controls
	9.4	Step 4: Develop Recovery Strategies
	9.5	Step 5: Develop IT Contingency Plan
	9.6	Step 6: Plan Testing, Training, and Exercises
	9.7	Step 7: Plan Maintenance
Risk Management	10.1	Risk Assessment
	10.2	Risk Mitigation
	10.3	Evaluation and Assessment
Certification, Accreditation, and Security Assessments	11.1	Certification, Accreditation, and Security Assessments Roles and Responsibilities
	11.2	Delegation of Roles
	11.3	The Security Certification and Accreditation Process
	11.4	Security Certification Documentation
	11.5	Accreditation Decisions
	11.6	Continuous Monitoring
	11.7	Program Assessments
Security Services and Products Acquisition	12.1	Information Security Services Life Cycle
	12.2	Selecting Information Security Services
	12.3	Selecting Information Security Products
	12.4	Security Checklists for IT Products
	12.5	Organizational Conflicts of Interest
Incident Response	13.1	Preparation
	13.2	Detection and Analysis
	13.3	Containment, Eradication, and Recovery
	13.4	Post-Incident Activity
Configuration Management	14.1	Configuration Management in the System Development Life Cycle
	1.42	Configuration Management Roles and Responsibilities.

IV. System Level Control Evaluation (Sampled Systems)

NIST FIPS 200 Controls and NIST SP 800-53		
FIPS 200 Family	**Number**	**Name**
Access Control	AC-1	Access Control Policy and Procedures
	AC-2	Account Management
	AC-3	Access Enforcement
	AC-4	Information Flow Enforcement
	AC-5	Separation of Duties
	AC-6	Least Privilege
	AC-7	Unsuccessful Login Attempts
	AC-8	System Use Notification
	AC-9	Previous Logon Notification
	AC-10	Concurrent Session Control
	AC-11	Session Lock
	AC-12	Session Termination
	AC-13	Supervision and Review – Access Control
	AC-14	Permitted Actions w/o Identification or Authentication
	AC-15	Automated Marking
	AC-16	Automated Labeling
	AC-17	Remote Access
	AC-18	Wireless Access Restrictions
	AC-19	Access Control for Portable and Mobile Systems
	AC-20	Personally Owned Information Systems
Awareness and Training	AT-1	Security Awareness and Training Policy and Procedures
	AT-2	Security Awareness
	AT-3	Security Training
	AT-4	Security Training Records
Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures
	AU-2	Auditable Events
	AU-3	Content of Audit Records
	AU-4	Audit Storage Capacity
	AU-5	Audit Processing
	AU-6	Audit Monitoring, Analysis, and Reporting
	AU-7	Audit Reduction and Report Generation
	AU-8	Time Stamps
	AU-9	Protection of Audit Information
	AU-10	Non-repudiation
	AU-11	Audit Retention
Certification, Accreditation, and Security Assessments	CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures
	CA-2	Security Assessments
	CA-3	Information System Connections
	CA-4	Security Certification
	CA-5	Plan of Action and Milestones
	CA-6	Security Accreditation
	CA-7	Continuous Monitoring

NIST FIPS 200 Controls and NIST SP 800-53		
FIPS 200 Family	**Number**	**Name**
Configuration Management	CM-1	Configuration Management Policy and Procedures
	CM-2	Baseline Configuration
	CM-3	Configuration Change Control
	CM-4	Monitoring Configuration Changes
	CM-4	Access Restrictions for Change
	CM-5	Access Restrictions for Change
	CM-6	Configuration Settings
	CM-7	Least Functionality
Contingency Planning	CP-1	Contingency Planning Policy and Procedures
	CP-2	Contingency Plan
	CP-3	Contingency Training
	CP-4	Contingency Plan Testing
	CP-5	Contingency Plan Update
	CP-6	Alternate Storage Sites
	CP-7	Alternate Processing Sites
	CP-8	Telecommunication Services
	CP-9	Information System Backup
	CP-10	Information System Recovery and Reconstitution
Identification and Authentication	IA-1	Identification and Authentication Policy and Procedures
	IA-2	User Identification and Authentication
	IA-3	Device Identification and Authentication
	IA-4	Identification Management
	IA-5	Authenticator Management
	IA-6	Authenticator Feedback
	IA-7	Cryptographic Module Authentication
Incident Response	IR-1	Incident Response Policy and Procedures
	IR-2	Incident Response Training
	IR-3	Incident Response Testing
	IR-4	Incident Handling
	IR-5	Incident Monitoring
	IR-6	Incident Reporting
	IR-7	Incident Response Assistance
Maintenance	MA-1	System Maintenance Policy and Procedures
	MA-2	Periodic Maintenance
	MA-3	Maintenance Tools
	MA-4	Remote Maintenance
	MA-5	Maintenance Personnel
	MA-6	Timely Maintenance
Media Protection	MP-1	Media Protection Policy and Procedures
	MP-2	Media Access
	MP-3	Media Labeling
	MP-4	Media Storage
	MP-5	Media Transport
	MP-6	Media Sanitization
	MP-7	Media Destruction and Disposal
Physical &	PE-1	Physical and Environmental Protection Policy and Procedures

NIST FIPS 200 Controls and NIST SP 800-53		
FIPS 200 Family	**Number**	**Name**
Environmental Protection	PE-2	Physical Access Authorization
	PE-3	Physical Access Control
	PE-4	Access Control for Transmission Medium
	PE-5	Access Control for Display Medium
	PE-6	Monitoring Physical Access
	PE-7	Visitor Control
	PE-8	Access Logs
	PE-9	Power Equipment and Power Cabling
	PE-10	Emergency Shutoff
	PE-11	Emergency Power
	PE-12	Emergency Lighting
	PE-13	Fire Protection
	PE-14	Temperature and Humidity Controls
	PE-15	Water Damage Protection
	PE-16	Delivery and Removal
	PE-17	Alternative Work Site
Security Planning	PL-1	Security Planning Policy and Procedures
	PL-2	System Security Plan
	PL-3	System Security Plan Update
	PL-4	Rules of Behavior
	PL-5	Privacy Impact Assessment
Personnel Security	PS-1	Personnel Security Policies and Procedures
	PS-2	Position Categorization
	PS-3	Personnel Screening
	PS-4	Personnel Termination
	PS-5	Personnel Transfer
	PS-6	Access Agreements
	PS-7	Third-Party Personnel Security
	PS-8	Personnel Sanctions
Risk Assessment	RA-1	Risk Assessment Policy and Procedures
	RA-2	Security Categorization
	RA-3	Risk Assessment
	RA-4	Risk Assessment Update
	RA-5	Vulnerability Scanning
System and Services Acquisition	SA-1	System and Services Acquisition Policy and Procedures
	SA-2	Allocation of Resources
	SA-3	Life Cycle Support
	SA-4	Acquisitions
	SA-5	Information System Documentation
	SA-6	Software Usage Restrictions
	SA-7	User Installed Software
	SA-8	Security Design Principles
	SA-9	Outsourced Information System Services
	SA-10	Developer Configuration Management
	SA-11	Developer Security Testing
System and	SC-1	System and Communications Protection Policy and Procedures

NIST FIPS 200 Controls and NIST SP 800-53		
FIPS 200 Family	**Number**	**Name**
Communications Protection	SC-2	Application Partitioning
	SC-3	Security Function Isolation
	SC-4	Information Remnants
	SC-5	Denial of Service Protection
	SC-6	Resource Priority
	SC-7	Boundary Protection
	SC-8	Transmission Integrity
	SC-9	Transmission Confidentiality
	SC-10	Network Disconnect
	SC-11	Trusted Path
	SC-12	Cryptographic Key Establishment and management
	SC-13	Use of Validated Cryptography
	SC-14	Public Access Protections
	SC-15	Collaborative Computing
	SC-16	Transmission of Security Parameters
	SC-17	Public Key Infrastructure Certificates
	SC-18	Mobile Code
	SC-19	Voice Over Internet Protocol
System and Information Integrity	SI-1	System and Information Integrity Policy and Procedures
	SI-2	Flaw Remediation
	SI-3	Malicious Code Protection
	SI-4	Intrusion Detection Tools and Techniques
	SI-5	Security Alerts and Advisories
	SI-6	Security Functionality Verification
	SI-7	Software and Information Integrity
	SI-8	Spam and Spy ware Protection
	SI-9	Information Input Restrictions
	SI-10	Information Input Accuracy, Completeness and Validity
	SI-11	Error Handling
	SI-12	Information Output Handling and Retention