BASELINE INFORMATION SECURITY STANDARDS: AN AUDIT PERSPECTIVE

Presented to:

Computer Security and Privacy Advisory Board

By:

Mr. Russell A. Rau

Assistant Inspector General for Audits, FDIC

June 13, 2002

PRESENTATION OUTLINE

- Information Security Risks
- Statutory Framework
- Program Level Security Standards
- Information Security Program Assessment Matrix
- System Level Security Standards
- Information System Assessment Matrix
- Summary

INFORMATION SECURITY RISKS

- Loss or Misuse of Resources
- Unauthorized Access to or Release of Sensitive Information
- Disruption of Critical Operations
- Inadvertent or Intentional Modification or Destruction of Data
- Embarrassment

INFORMATION SECURITY RISKS

- Complexity and interconnectivity
- Speed and accessibility
- Standardization
- Physical threats
- Availability of hacking tools
- Exclusive reliance on computer controls
- Expectations

INFORMATION SECURITY RISKS

- Audits and Evaluations
  - Increasingly important aspect of management control
  - Critical to ensuring confidentiality, integrity and availability of information
  - Difficult to perform financial or performance audits without considering information security (Audit Standards)
  - Government Information Security Reform Act

STATUTORY FRAMEWORK

- Government Information Security Reform - FY 2001 DOD Authorization Act
  - Promotes information security as an integral part of business operations
  - Requires information security program and plan practiced throughout system life cycle
  - Focuses on training, incident response, internal monitoring, and independent external evaluation

STATUTORY FRAMEWORK

- OMB identified six common weaknesses
  - Senior Management Attention
  - Performance Measurement
  - Security Education and Awareness
  - Funding and Integrating Security into Capital Planning and Investment Control
  - Contractor Security
  - Intrusion Detection/Incident Response
- Next report due September 16, 2002

STATUTORY FRAMEWORK

- H.R. 3844, Federal Information Security Management Act of 2002
  - Defines "Information Security" in terms of integrity, confidentiality and availability
  - Requires agency-wide information security program, including other agencies, contractors, and "sources"
    - Continued emphasis on risk assessment and cost-effectiveness
    - Compliance with security standards and guidelines

STATUTORY FRAMEWORK

- Sets milestones for submission of National Institute of Standards and Technology (NIST) standards, guidelines and minimum information security requirements to OMB
  - Categorization of information and systems
  - Detection and response to security incidents
- Establishes within NIST an Office of Information Security Program
- Establishes Information Security Advisory Board

STATUTORY FRAMEWORK

- Annual independent evaluations by Inspectors General starting March 1, 2003
  - Performed in accordance with Government Auditing Standards

PROGRAM LEVEL SECURITY STANDARDS

- OMB Circular A-130 Defines Adequate Security:

  “Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational and technical controls.”

PROGRAM LEVEL SECURITY STANDARDS

- OMB Circular A-123 Discusses Reasonable Assurance:

  “Management controls must provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. Management controls developed for agency programs should be logical, applicable, reasonably complete, and effective and efficient in accomplishing management objectives.”

PROGRAM LEVEL SECURITY STANDARDS

- OIG Evaluated Establishment and Implementation of Management Controls
- Three Assurance Categories
  - Reasonable Assurance: Management controls provide reasonable, but not absolute, assurance of adequate security
  - Limited Assurance: Management controls partially effective but do not provide reasonable assurance of adequate security
  - No Assurance: No assurance of adequate security

INFORMATION SECURITY PROGRAM ASSESSMENT MATRIX

Assessment of the FDIC’s Information Security Program 2001 - 2002				
	2001		2002	
Management Control Areas	**Rating for Establishment of Controls**	**Rating for Implementation of Controls**	**Rating for Establishment of Controls**	**Rating for Implementation of Controls**
Risk Management *(OMB Question C.1)*	🟢 Reasonable	🟡 Limited		
Systems Security *(OMB Question D.1)*	🟡 Limited	🟡 Limited		
Security Training *(OMB Question D.1)*	🟡 Limited	🔴 None		
Incident Response Reporting *(OMB Question B.5)*	🟡 Limited	🟡 Limited		
Capital Planning and Investment Control *(OMB Question D.3)*	🟡 Limited	🔴 None		

INFORMATION SECURITY PROGRAM ASSESSMENT MATRIX

	2001		2002	
Management Control Areas	**Rating for Establishment of Controls**	**Rating for Implementation of Controls**	**Rating for Establishment of Controls**	**Rating for Implementation of Controls**
Protection of Critical Assets *(OMB Question B.4)*	🟡 Limited	🟡 Limited		
Performance Measurement *(OMB Question B.2)*	🔴 None	🔴 None		
Integration of Activities *(OMB Question B.3)*	🟡 Limited	🟡 Limited		
Contractor/External Security *(OMB Question C.2 and D.2)*	Not Rated	Not Rated		
Responsibilities and Authority *(OMB Question B.1)*	(Not applicable)			
Overall Assessment	🟡 (Limited)			

SYSTEM LEVEL SECURITY STANDARDS

- OMB Circular A-130, Appendix III
  - Security of Federal Automated Information Resources
- NIST Special Publication 800-26
  - Security Self-Assessment Guide of Information Technology Systems
- GAO Federal Information System Control Audit Manual
- Statutes, Regulations, and Other Guidance

SYSTEM LEVEL SECURITY STANDARDS

- OMB Circular A-130
  - Assignment of Security Responsibilities
  - Security Planning and Review
    - Rules of Behavior
    - Training
    - Personnel Controls
    - Incident Response
    - Continuity of Support
    - Technical Security
    - System Interconnection
  - Authorization to Process
- GAO FISCAM
  - Segregation of Duties
  - Service Continuity
  - Software Development and Change Control
  - Access Control
  - System Software Controls

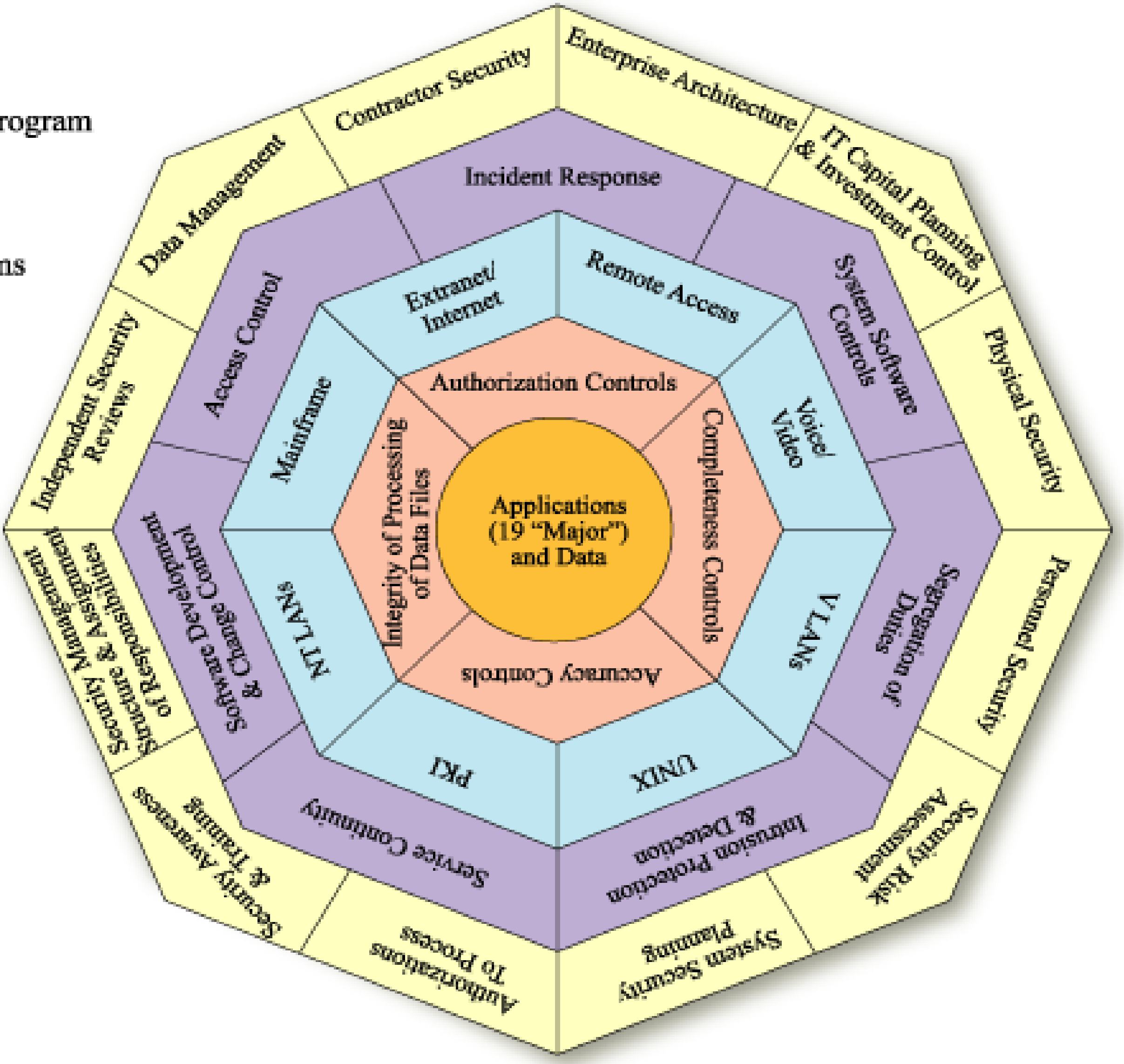
SYSTEM LEVEL SECURITY STANDARDS

- OMB Circular A-130
  - Enterprise Architecture
  - Capital Planning and Investment Control Process

- GAO FISCAM
  - Entity-Wide Information Security Program

Information Security Environment

- 🟨 Entity-Wide Security Program
- 🟪 General Controls
- 🟦 General Support Systems
- 🟥 Application Controls
- 🟧 Applications and Data



Contractor Security

Enterprise Architecture

IT Capital Planning & Investment Control

Physical Security

Personnel Security

Security Risk Assessment

System Security Planning

Authorizations To Process

Security Awareness & Training

Security Management Structure & Assignment of Responsibilities

Independent Security Reviews

Data Management

Incident Response

System Software Controls

Segregation of Duties

Intrusion Protection & Detection

Service Continuity

Software Development & Change Control

Access Control

Extranet/ Internet

Remote Access

Voice/ Video

VLANs

UNIX

PKI

NT LANs

Mainframe

Authorization Controls

Completeness Controls

Accuracy Controls

Integrity of Processing of Data Files

Applications (19 "Major") and Data

SYSTEM LEVEL SECURITY MATRIX

- Together with Color-Coding, Focuses Attention on Security Issues
- Reflects Interrelated Nature of Security Challenge
- Identifies Gaps in Coverage
- Valuable in Risk Assessments

SYSTEM LEVEL SECURITY MATRIX

- Depth of Coverage in Each Area
  - For Example: Security Risk Assessment
    - Classification of Information Resources
    - Identification of Major Applications
    - Security Planning
    - Security Reviews
    - Authorization of Processing
    - Assignment of Security Responsibility

SUMMARY

- GISRA Lessons Learned
  - Partnership with the Chief Information Officer
  - Multi-year, Top-Down Approach
  - Program Management Philosophy
  - Focus on Business Operations
  - Emphasis on Long-Term Solutions, not Quick Fixes
  - Development of OIG Capabilities

SUMMARY

- CAUTIONS
  - Proliferation of Guidance
    - Regulatory Requirements
    - Federal and Commercial Security Assessment Tools
    - Other Publications
  - Overlapping Review Coverage
    - Impact on CIO Resources and Operations