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

- 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

  - 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
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.”
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.”
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

<table>
<thead>
<tr>
<th>Management Control Areas</th>
<th>2001</th>
<th>2002</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rating for Establishment of Controls</td>
<td>Rating for Implementation of Controls</td>
</tr>
<tr>
<td>Risk Management <em>(OMB Question C.1)</em></td>
<td><img src="Image" alt="Reasonable" /></td>
<td><img src="Image" alt="Limited" /></td>
</tr>
<tr>
<td>Systems Security <em>(OMB Question D.1)</em></td>
<td><img src="Image" alt="Limited" /></td>
<td><img src="Image" alt="Limited" /></td>
</tr>
<tr>
<td>Security Training <em>(OMB Question D.1)</em></td>
<td><img src="Image" alt="Limited" /></td>
<td><img src="Image" alt="None" /></td>
</tr>
<tr>
<td>Incident Response Reporting <em>(OMB Question B.5)</em></td>
<td><img src="Image" alt="Limited" /></td>
<td><img src="Image" alt="Limited" /></td>
</tr>
<tr>
<td>Capital Planning and Investment Control <em>(OMB Question D.3)</em></td>
<td><img src="Image" alt="Limited" /></td>
<td><img src="Image" alt="None" /></td>
</tr>
</tbody>
</table>
## INFORMATION SECURITY PROGRAM ASSESSMENT MATRIX

<table>
<thead>
<tr>
<th>Management Control Areas</th>
<th>2001</th>
<th>2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Critical Assets <em>(OMB Question B.4)</em></td>
<td><img src="Image" alt="Limited" /></td>
<td><img src="Image" alt="Limited" /></td>
</tr>
<tr>
<td>Performance Measurement <em>(OMB Question B.2)</em></td>
<td><img src="Image" alt="None" /></td>
<td><img src="Image" alt="None" /></td>
</tr>
<tr>
<td>Integration of Activities <em>(OMB Question B.3)</em></td>
<td><img src="Image" alt="Limited" /></td>
<td><img src="Image" alt="Limited" /></td>
</tr>
<tr>
<td>Contractor/External Security <em>(OMB Question C.2 and D.2)</em></td>
<td>Not Rated</td>
<td>Not Rated</td>
</tr>
<tr>
<td>Responsibilities and Authority <em>(OMB Question B.1)</em></td>
<td>(Not applicable)</td>
<td></td>
</tr>
<tr>
<td><strong>Overall Assessment</strong></td>
<td><img src="Image" alt="Limited" /></td>
<td>(Limited)</td>
</tr>
</tbody>
</table>
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
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