



# House Bill 2935

Office of State Finance

July 2006



# Agenda

## House Bill 2935

- Welcome
- Background
- Changes in Inventory and Annual Planning Processes
- Security
  - Disclosure of Information
  - Enforcement of Minimum Standards
  - Risk Assessment
- Questions and Answers



# Background

House Bill 2935

- **Security**
  - Legislative Concern
- **New Provision**
  - Inventory
  - Data Processing Plans
- **Clean Up Bill**
  - Terminology
  - New Technology
  - Outdated Provisions
  - Protection of Infrastructure



# Inventory

## House Bill 2935

- Types of items
  - Application systems, systems software, hardware, technology equipment, communication or telecommunication equipment owned, leased or rented for use in communication services for state government
- Dollar Value
  - \$500 individual items
- Due Date
  - September 1<sup>st</sup>



# Disaster Recovery Plans

House Bill 2935

- Due Date
  - September 1<sup>st</sup>



# Annual Operating Plans

House Bill 2935

- Background and History
  - Awkward
  - Tied to Budget Process
  - Data Processing – Telecom Plans due at Different Times
  - 9 months before Approved Budget
  - Updated after Budget Approved
  - Labor Intensive
  - Who Used Report



# Annual Operating Plans - - Continued

House Bill 2935

- New Process
  - Annual Operating Plan
  - Consolidated Plan
  - Expenditure Planned by Defined Categories
  - Actual Expenditure Recorded by Defined Categories
  - Object Codes (Chart of Accounts) Updated
  - Plan by Project



# Annual Operating Plans - - Continued

House Bill 2935

- Due Date
  - Planning Templates – January 1, 2007
  - First Plan – July 1, 2007



# Security

House Bill 2935

- Disclosure of Information
  - Confidential by State or Federal Statute
  - Information Technology System Details
  - Information Affecting
    - Personal Identity
    - Personal Security
    - Physical Security of State Assets



# Minimum Information Security and Internal Control Standards

House Bill 2935

- Enforcement Team
  - Office of State Finance
  - Office of Homeland Security
  - Oklahoma State Bureau of Investigation
- Process
  - Agency Notified of Non-Compliance
  - Agency Submits Plan to Become Compliant



# Minimum Information Security and Internal Control Standards - - Continued

House Bill 2935

- **Process** (continued)
  - **Non-Compliance Process**
    - Extend Time Frame
    - Assist Agency
    - Notification of agency removal from State's infrastructure
    - Notification of Enforcement Team to take Control of Agency Information Technology Function
    - Recommend to Governor and Legislature Agency Information Technology Function Transfer to Another State Agency



# Risk Assessment

House Bill 2935

- Background
  - Legislative Committee Meeting
    - Presentation by Homeland Security and FBI
    - Status of State's Information Security
- Legislation
  - Create Standard Security Risk Assessment Document
  - Comply with
    - ISO/IEC 17799 Standard
    - NIST SP800-30



# Risk Assessment - - Continued

## House Bill 2935

- Legislation (Continued)
  - Select Risk Assessment Firms
  - December 1<sup>st</sup> – Agency Risk Assessment Report
  - January 1<sup>st</sup> – Governor and Legislature Report
- Purpose
  - Identify and Prioritize Information Security Vulnerabilities
  - Establish an Agency Information Security Baseline
  - Define Recommendations to Mitigate Vulnerabilities



# Risk Assessment - - Continued

House Bill 2935

- Process
  - Define the Standard Security Risk Assessment Document
    - Confidentiality
    - Integrity
    - Availability
  - Standard Security Control Category Safeguards
    - Management
    - Operational
    - Technical



# Risk Assessment - - Continued

House Bill 2935

- Recognition of State Agency Differences
  - Business Information
    - Mission/Function
    - Services
    - Data Collected and Maintained
    - Customer Profile
    - Number of Personnel
    - Funding



# Risk Assessment - - Continued

House Bill 2935

- Recognition of State Agency Differences  
(Continued)
  - Technology Information
    - Operating Systems
    - Types of Hardware
    - Networks and Equipment
    - Security Solutions
    - Internet Infrastructure



# Risk Assessment - - Continued

House Bill 2935

- Recognition of State Agency Differences  
(Continued)
  - Categorize Agency Risk Based on Profile
    - Low
    - Medium
    - High
  - Tailor Risk Assessment Questions Based on Risk Category



# Risk Assessment - - Continued

House Bill 2935

- Current Status
  - Finalizing Agency Profile Document
  - Selecting Software Tool
  - Finalizing RFP to Select Risk Assessment Consulting Firms
    - Include Profiling Questionnaire
    - Include Risk Assessment Document by Risk Category
    - Options (Penetration Testing)



# Risk Assessment - - Continued

House Bill 2935

- Next Steps
  - Distribute Agency Profile Document
  - Finalize Risk Assessment Document
  - Distribute Risk Assessment Document to Agencies
  - Release RFP
  - Select Risk Assessment Vendors
  - Activate Software Tool
  - OSF Assist Agencies
  - Agency Decide on Self Assessment or Consultant
  - OSF Define Final Report Format



# Questions

## House Bill 2935

- Do we need to submit Information Technology and Telecommunication inventories this year?
  - *Yes. The inventories are due on September 1, 2006.*
- Do we need to submit Disaster Recovery Plans this year?
  - *Yes. The Disaster Recovery Plans are due on September 1, 2006.*



# Questions

## House Bill 2935

- Do we have to submit the three-year strategic Information Technology and Telecommunications Plans?
  - *No. The three-year strategic plans submitted in September and October 2005 will be used by OSF to approve requested purchases for the period from July 2006 to June 2007.*



# Questions

## House Bill 2935

- When will instructions for completing the one-year operating plans be available?
  - *The plan is to have these instructions to the agencies by January 1, 2007.*



# Questions

## House Bill 2935

- When can we see the Standard Risk Assessment?
  - *The Agency Profile Document will be distributed by the end of the week.*
- Who are the Risk Assessment Firms?
  - *The firms will be selected based on the RFP responses. I anticipate the RFP will be released by the end of July and vendors selected by end of August.*



# Questions - - Continued

## House Bill 2935

- How do we get help, if we don't understand the question?
  - *Contact the OSF Help Desk at 405-521-2444 or 1-866-521-2444 or [helpdesk@osf.ok.gov](mailto:helpdesk@osf.ok.gov). The Help Desk will answer your question or route it to the appropriate OSF person who will respond to you. All questions will be logged by the Help Desk for analysis and to ensure you receive a timely response.*



# Questions - - Continued

## House Bill 2935

- Do we have to use a consultant?
  - *No, each agency has to decide if their agency has the expertise to respond to Standard Risk Assessment Document or wants to use a risk assessment consultant*
- Will OSF complete the Risk Assessment Document for agencies it supports?
  - *OSF will assist each agency it supports to complete the portions of the Risk Assessment Document related to the areas it supports. The agency will have to complete the other sections of the Risk Assessment Document.*



## Questions - - Continued

### House Bill 2935

- When can we start?
  - *Complete the profile as soon as you receive it. You can begin the self assessment when the document and software tool are available. If you plan to use a consultant, you will have to wait until the risk consulting firms are selected.*



## Questions - - Continued

### House Bill 2935

- Will the consultants have to answer the Standard Risk Assessment questions?
  - *Yes. We will require each consultant to issue a report to the agency and to answer the questions specific to the agency's risk category (low, medium, high). By having the questions answered for each agency, OSF will be able to prepare summary information for the report to the Governor and Legislature.*



## Questions - - Continued

### House Bill 2935

- Will the result of the risk assessment be available to the public?
  - No, the report prepared and results of the risk assessment will contain information that is confidential. If the risk assessment results are disclosed, it could affect personal security, personal identity or the physical security of State assets.



## Questions - - Continued

### House Bill 2935

- Are there funds available for the third-party assessment and to mitigate the identified vulnerabilities?
  - *As far as we know no funds were appropriated for the third-party assessment or to fix the identified vulnerabilities. This initial risk assessment is a first step in the process to identify vulnerabilities and to define the steps needed to be taken by agencies to mitigate the vulnerabilities identified.*



# Questions

House Bill 2935

- Questions