

IT Council Security Updates and Document Approvals

Presented by the
CA State Information Security Office
10/19/07

State's IT Strategic Plan

Goal 3 – Ensure State Information Assets are Secured and Privacy Protected

Tasks Completed and Requesting Your Approval:

- Goal 3, Objective 1, Action 1 – Update the IT Security Program Guideline
- Goal 3, Objective 2, Action 3 – Develop a methodology and a set of tools that departments can use to self-assess their IT security vulnerabilities
- Goal 3, Objective 3, Action 2 – Develop and publish a document that outlines the general roles and responsibilities assigned to an agency's Information Security Officer.

Vetting Process

- Workgroups
- Subject Matter Expert Reviews
- Posted to State Information Security Office's (SISO) Web Site for Vetting (minimum 2 weeks)
- Feedback reviewed and incorporated
- In some cases, re-posted for additional vetting
- Shared with select groups for further input

Information Security Program Guide for State Agencies

Goal 3, Objective 1, Action 1

- Updated, enhanced, and added content including:
 - Title Renamed
 - Includes A Suggested Implementation Strategy
 - 12 Security Components (previously only 10)
 - Glossary

Risk Assessment Toolkit

Goal 3, Objective 2, Action 3

- Web Page
- Contains assessment tools from basic to advanced, including statutory
- Tools: reports, charts, matrix, project methodology, audit guides

Guide for the Role and Responsibilities of an Information Security Officer Within State Government

Goal 3, Objective 3, Action 2

- Policy requirements for an ISO
- Necessary ISO skills and abilities
- ISO role and responsibilities in the 12 security components
- Glossary

Coming Soon!

The following Action Items will be ready for approval at the next IT Council Meeting:

- Goal 3, Objective 1, Action 3 – Develop a general Internet Usage Policy and a related best practice guideline for agencies.
- Goal 4, Objective 5, Action 3 - Establish consistency between operational recovery and COOP/COG planning efforts to align processes, terminology and reporting requirements.

Questions?