



CALIFORNIA OFFICE OF  
INFORMATION SECURITY  
& PRIVACY PROTECTION



# Transforming the Future

## Strategic Plan & Policy Development

---

Meeting

June 19, 2009



# Presentation Objectives

---

- Provide overview of Strategic Vision for Office of Information Security
- Provide forum for information sharing on the strategic plan
- Present overview of Policy Project



# Overview of Presentation

---

- Strategic Vision
- History of OIS Strategic Plan Development Project
- Overview of the IT Strategic Plan Strategic Concepts
- OIS Strategic Concepts in Relation to IT Strategic Plan
- Next Steps on the Strategic Plan Development
- Q&A

---

Break

---

- Overview of Policy Refresh Project
- Current State of the Policy Project
- Vetting & Review Process
- Q&A and Wrap Up

# Strategic Vision

---



# History of OIS Strategic Plan Development Project

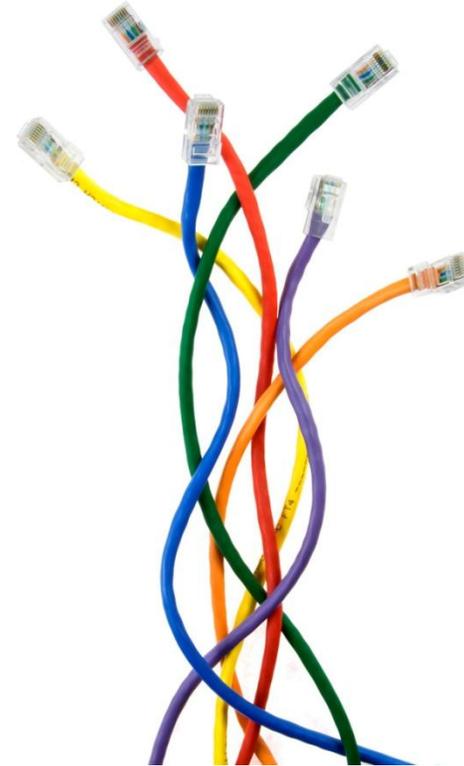
---



# Key Inputs to Strategic Plan

---

- Visioning sessions with key OIS stakeholders
- Industry Research
- Agency Workshops
- Federal Inputs



# Key Findings – Internal View

---

- Enterprise Risk Management
  - Need enterprise standard for security and privacy metrics
  - Enterprise view of security/privacy health of the state
- Policy and Standards development
  - Particularly in areas where agencies need guidance
- Risk-based enforcement
  - Prioritize based on greatest areas of risk
  - Tools, resources and technology to scale up operations





# Key Findings – Agency View

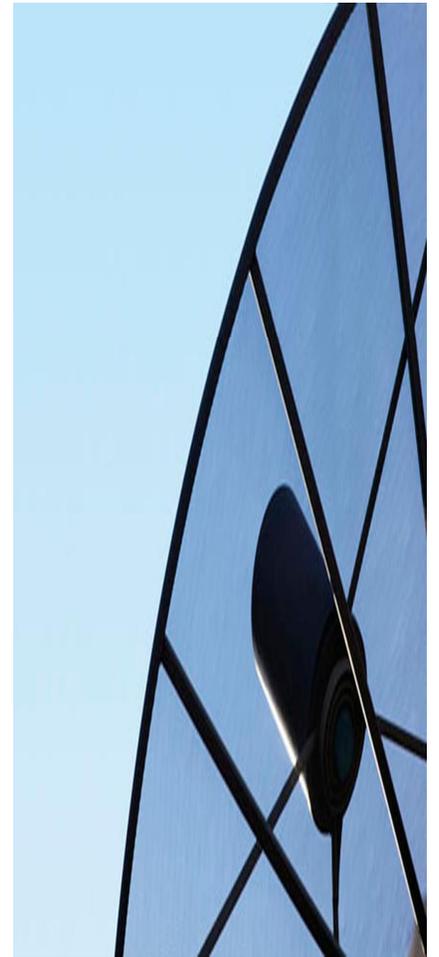
---

- ❑ **Policy and Standards:** Agencies need clear, consistent, well-communicated policies and standards
- ❑ **Training & Awareness:** Need for more awareness training across the board, and technical security at all levels
- ❑ **Access Control:** Challenges in managing identities, credentials, authentication
- ❑ **Data lifecycle/Content Management:** Identifying where data is located and how to protect it
- ❑ **Privacy:** Unclear on definitions of privacy and personal information, and how to handle it from ‘cradle to grave’ to comply with policy and regulations

# Federal-Level Inputs

*Securing Cyberspace for the 44<sup>th</sup> Presidency* (CSIS Report), recommended a comprehensive strategy for security in cyberspace. Cyberspace is a vital asset for national security, public safety, economic prosperity, and the delivery of critical services to the public.

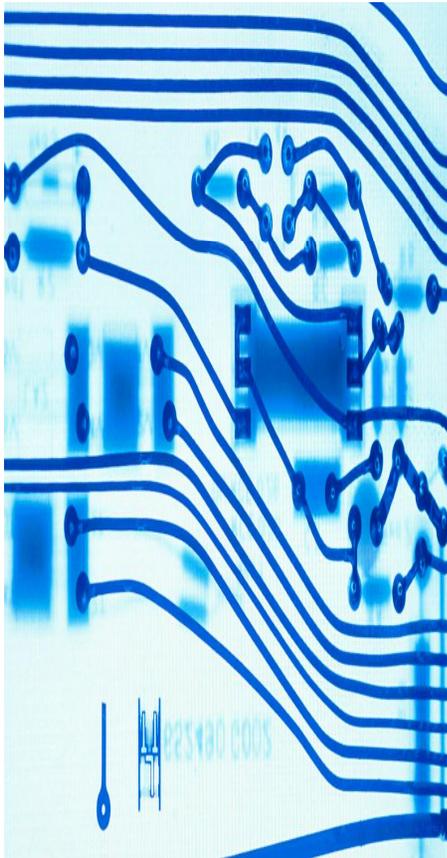
- CSIS Commission on Cybersecurity for the 44<sup>th</sup> Presidency, *Securing Cyberspace for the 44<sup>th</sup> Presidency*, December 2008



# Federal-Level Inputs

---

Director of National Intelligence:



- “[T]he growing connectivity between information systems, the Internet, and other infrastructure creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures.”
  - *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record, March 10, 2009, at 39.*

# Federal-Level Inputs

---

## *Cyberspace Policy Review (Hathaway Report)*

- “The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local and tribal governments, the private sector, and international allies to significant incidents.”
  - *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*





# Application of Key Findings

---

- Analyzed and synthesized these inputs and drafted 5 Strategic Concepts (with associated goals and objectives) as the basis for addressing the identified needs/gaps
- Included input and direction from meetings with the OCIO for alignment with the IT Strategic Plan
- OIS has been consolidated into the OCIO as part of the Governor's Reorganization Plan

# IT Strategic Plan

---

- Issued January 15, 2009
- Governor's Reorganization Plan took effect on May 10, 2009



California  
Information  
Technology  
Strategic  
Plan

January 15

2009

---

Strategic Concepts, Strategies, & Goals  
Volume 1

Arnold Schwarzenegger  
Governor

Teri Takai  
Chief Information Officer



# IT Strategic Plan – Strategic Concepts

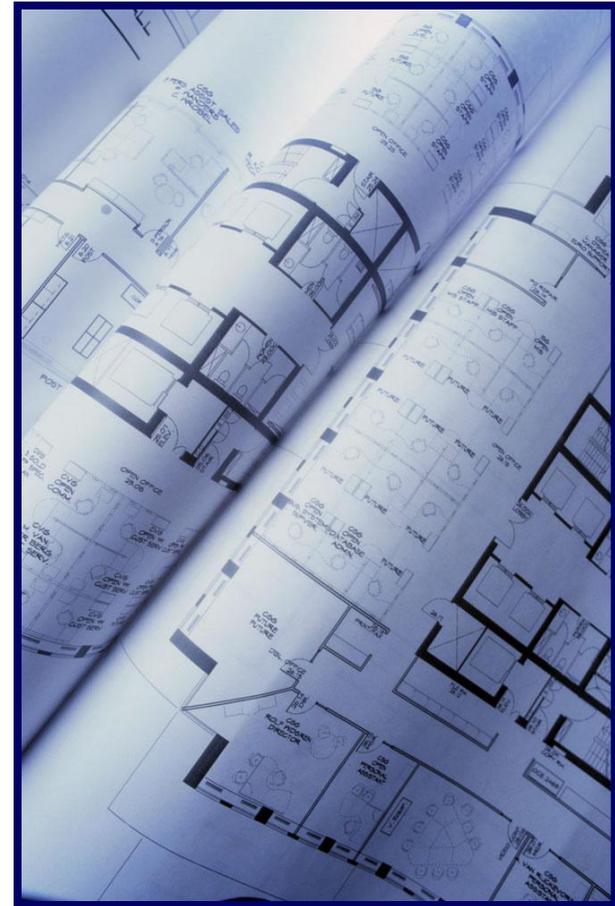
---

1. IT as Reliable as Electricity
2. Fulfilling Technology's Potential to Transform Lives
3. Self-governance in the Digital Age
4. Information as an Asset
5. Economic and Sustainable
6. Facilitating Collaboration that Breeds Better Solutions

# OIS Strategic Concepts

---

- Each of Five OIS Strategic Concepts relates to one or more IT Strategic Concepts
- OIS Goals are Aligned to IT Goals
- IT Goals are Aligned to State Needs





IT as reliable as Electricity	Fulfilling technologies potential to transform lives	Information as an Asset	Self-governance in the Digital Age	Economic and sustainable	Facilitating collaboration that breeds better solutions
<p align="center"><u>OIS Strategic Concept</u></p> <p><b>A Digital Infrastructure that is Resilient, Secure and Trustworthy</b></p>	<p align="center"><u>OIS Strategic Concept</u></p> <p><b>Make Roaming the Internet as Safe as Roaming Your Neighborhood</b></p>		<p align="center"><u>OIS Strategic Concept</u></p> <p><b>A Secure, Trusted Identity for Every California Citizen</b></p>	<p align="center"><u>OIS Strategic Concept</u></p> <p><b>Security that Leads the Way to More Efficient Technology</b></p>	<p align="center"><u>OIS Strategic Concept</u></p> <p><b>Effective Security that Doesn't Impede Collaboration or Delivery of Services</b></p>
<p><b>Purpose:</b> Implement "state-of-the art" enterprise information security to combat and manage current and future cyber risks to California's enterprise IT infrastructure and the information housed within it.</p>	<p><b>Purpose:</b> Implement enterprise "information-centric" security solutions for the state whereby the security is always with the asset (information) regardless of where the information resides within the state's IT infrastructure.</p>		<p><b>Purpose:</b> Define a secure, trusted identity scheme in which California citizens, government employees and business partners have a single identity in which to interact online with California government irrespective of agency.</p>	<p><b>Purpose:</b> Leverage secure, trusted identity scheme to identify and eliminate areas of waste within the IT infrastructure leading to a greener environment.</p>	<p><b>Purpose:</b> Establish secure communication standards to support online collaboration between California state government, its business partners and other state governments.</p>

# 1: A Digital Infrastructure that is Resilient, Secure and Trustworthy

- Aligns with IT Strategic Concept: IT as Reliable as Electricity
- Purpose: Implement “state-of-the-art” enterprise information security to combat and manage current and future cyber risks to California’s enterprise IT infrastructure and the information housed within it.



## 2: Make Roaming the Internet as Safe as Roaming Your Neighborhood



- Aligned to IT Strategic Concepts:
  - Fulfilling technologies potential to transform lives
  - Information as an Asset
- Purpose: Implement enterprise “information-centric” security solutions for the state whereby the security is always with the asset (information) regardless of where the information resides within the state’s IT infrastructure.

# 3: A Secure, Trusted Identity for Every California Citizen

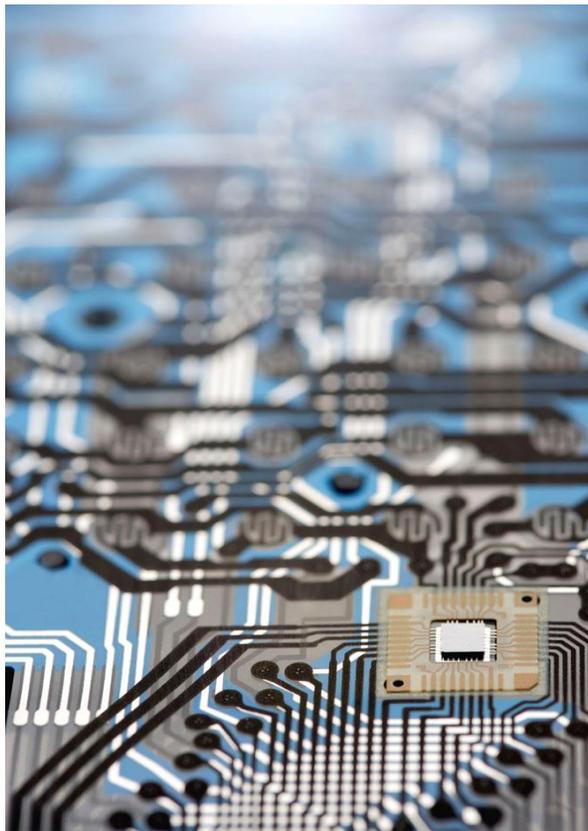
---

- Aligned to IT Strategic Concept: Self-governance in the Digital Age
- Purpose: Define a secure, trusted identity scheme in which California citizens, government employees and business partners have a single identity in which to interact online with California government irrespective of agency.



# 4: Security that Leads the Way to More Efficient Technology

---



- Aligned to IT Strategic Concept: Economic and Sustainable
- Purpose: Leverage secure, trusted identity scheme to identify and eliminate areas of waste within the IT infrastructure leading to a greener environment.

# 5: Effective Security that Doesn't Impede Collaboration or Delivery of Services

---

- Aligned to IT Strategic Concept: Facilitating collaboration that breeds better solutions
- Purpose: Establish secure communication standards to support online collaboration between California state government, its business partners and other state governments.



# Next Steps on the Strategic Plan Development

---

- Reviewed by OCIO and Key Stakeholders
- Final Stages of Revision/Review
- Final Publication planned July 2009



# Q&A on Strategic Plan

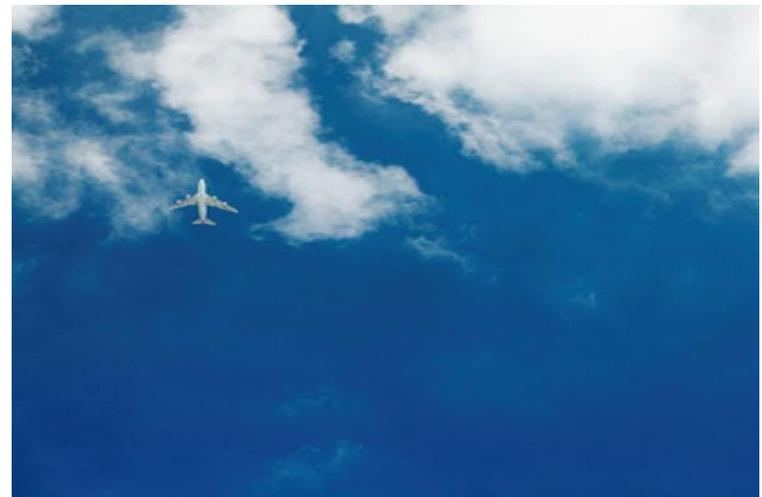
---



# Break

---

10 Minutes



# OIS Policy Project

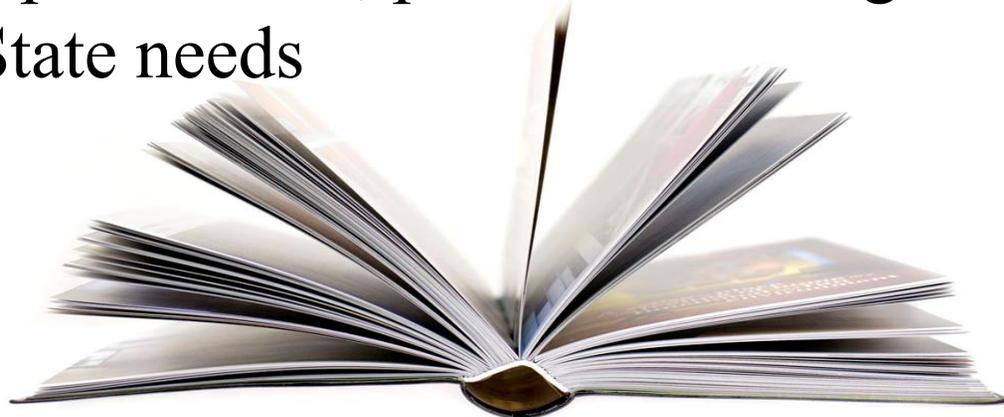
---



# Policy Project Overview

---

- Goal of Policy Project
  - Develop new and revise existing policies to address the current and future landscape of information security and privacy threats, risks, and vulnerabilities to the State
  - Develop standards, procedures and guidelines to meet State needs





# Terminology

---

- **Policy** - A high-level statement that describes mandatory or prohibited actions, applicable to individuals who fall within the scope of the policy, which aim to protect State information assets.
- **Standard** - A detailed published specification that contains measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy.



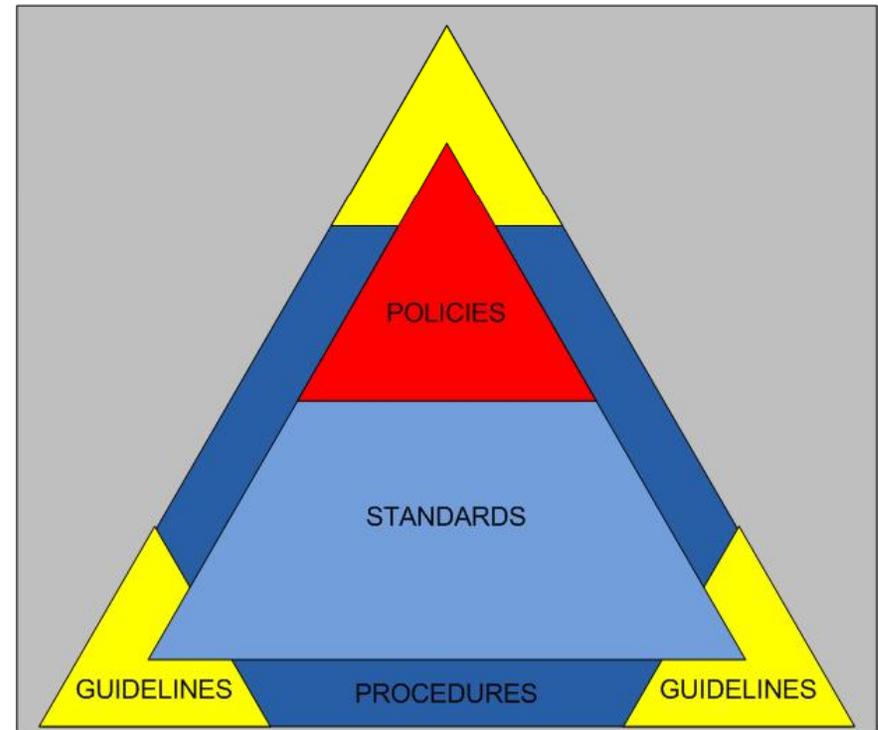
# Terminology – continued

---

- **Procedure** - A specific series of actions an individual must take in order to comply with policies and standards.
  
- **Guideline** - Recommended actions that describe leading practices which support policies, standards and procedures.

# How They Fit Together

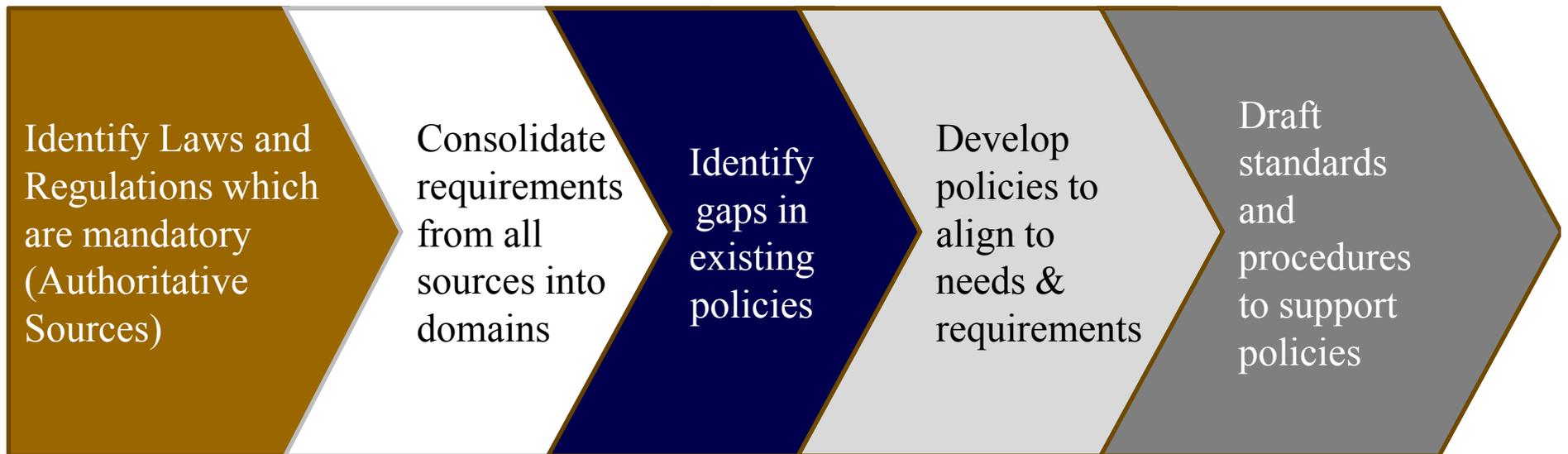
- **Policies** describe WHAT required actions to take from a HIGH-LEVEL
- **Standards** describe WHAT the DETAILED –LEVEL baseline requirements are for various technologies and configurations that are supported in the enterprise.
- **Procedures** may support both policies and standards and describe HOW to perform compliance activities.
- **Guidelines** may also support policies and standards, but are recommended leading practices on what to consider or HOW to perform security activities.



# Policy Development Process

---

- Five Step Process to Develop Applicable Policies for State



# Current State of Policy Project

---

- Drafting Policies, Standards, and Procedures
- Rolling Phases in this Process
  - Internal Agreement on Content
  - Initial Drafting and Revision
  - Vetting
  - Policy Review
  - Publishing
  - Training



# Information Security Policy

## Domains

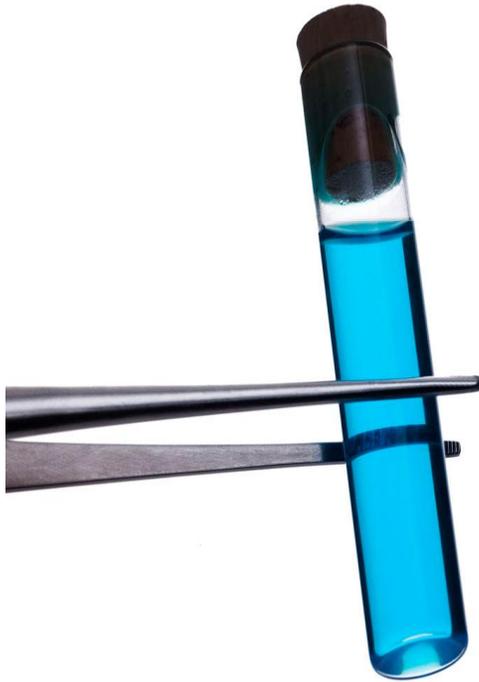
---

1. Risk Management
2. Policy Management
3. Security Organization
4. Asset Management
5. Human Resources Security
6. Physical and Environmental Security
7. Communications & Operations Management
8. Access Control
9. IS Acquisition, Development and Maintenance
10. Incident Management
11. Business Continuity/ Disaster Recovery
12. Compliance
13. Privacy

SAM Domain		Policies	Standards			Procedures
5305	Risk Management	2 Subsections				Risk Assessment Procedure
5310	Policy Management	3 Subsections				
5315	Organizing Information Security	1 Subsection				
TBD	Privacy	NEW	Notice to Individuals Standard	Individual Access to Privacy Data Standard		
5320	Information Asset Management	3 Subsections	Acceptable Use Standard Includes Internet, Email	Information Asset Classification Standard		
			3 <sup>rd</sup> Party Security Standard	Information Asset Handling Standard		
5325	Human Resources Security	3 Subsections	Information Security & Privacy Training Standard			
5330	Physical & Environmental Security	3 Subsections				
5335	Communications & Operations Management	3 Subsections	Vulnerability Management Standard	Logging Standard	Change Management Standard	
5340	Access Control	2 Subsections	User Access Management Standard	Password Management Standard		
5345	Information Systems Acquisition, Development & Maintenance	3 Subsections	Enterprise Security Architecture Standard	Configuration Management Standard	Use and Management of Encryption Standard	
			Telework Security Standard	System Development Lifecycle Standard		
5350	Incident Management	2 Subsections	Incident Response Standard			Incident Reporting Procedure
5355	Disaster Recovery & BCM	1 Subsection	Disaster Recovery Standard			Disaster Recovery Procedure
5360	Compliance	1 Subsection				Annual Compliance Reporting Procedure

# Vetting & Review Process

---



- Vetting
- Policy Review – Five Week Process
  - Executive Presentation
  - Executive Review
    - Agency/Department AIO/CIO/ISO Review
    - Submit through CIO/AIO for consistency
  - OCIO Feedback Review – may result in FAQ
  - OCIO Facilitated Review
  - ELC Conference Call
  - Informational Copy Release
  - Publish Policy

# OCIO Policy Review Process

## OCIO Policy Review Process

Wednesday, July 16, 2008

Policy Development  
and Vetting



# Publishing and Training

---



# Q&A

---



# Wrap Up/ Contact Information

---

- OIS Strategic Plan Issuing Shortly
- First Policies and Standards Vetting Shortly
- Contact OIS for more information:
  - Office of Information Security
  - [security@oispp.ca.gov](mailto:security@oispp.ca.gov)
  - (916) 445-5239

