



California
TECHNOLOGY AGENCY
Office of Information Security

Information Security Officer Meeting

March 14, 2013

Meeting Agenda

— Topics —

<u>Introductions/Opening Remarks</u>	9:30 - 9:35
<u>Statewide Security Program Updates</u> Project Update - Emergency Function 18, Cyber Security Annex Victoria Craig, California Technology Agency, Office of Information Security Policy Workgroup Update Patrick McGuire, California Technology Agency, Office of Information Security	9:35 - 10:35
<u>State Enterprise Architecture</u> Subbarao Mupparaju, Technology Agency, Enterprise Architecture	10:35 - 11:25
<u>Q&A and Closing</u>	11:25 - 11:30

Thanks for joining us!

Introductions/Opening Remarks

National Journal

America's 3 Biggest Cybersecurity Vulnerabilities

The Obama administration has put cyberattacks at the top of the global threats, and concerns are rising about at-risk infrastructure

by Matt Vasilogambros

Updated: March 13, 2013 | 4:32 p.m.
March 13, 2013 | 4:00 p.m.



Director of National Intelligence James Clapper (right) and FBI Director Robert Mueller No. 1 threat. (AP Photo/Susan Walsh)

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
Strategic insights and bipartisan policy solutions

Topics | Regions | Programs | Experts | Multimedia | Publications | Events

HOME / TOPICS / TECHNOLOGY / CYBERSECURITY

Cybersecurity

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine
March 13, 2013
NATIONAL RESEARCH COUNCIL
INSTITUTE OF MEDICINE
ACADEMY OF ENGINEERING

Professionalizing the Nation's Cybersecurity Workforce

STUDYING CYBERSECURITY

Defense and Security

the WHITE HOUSE PRESIDENT BARACK OBAMA
★ ★ ★ ★ THE WHITE HOUSE WASHINGTON ★ ★ ★ ★
BLOG PHOTOS & VIDEO BRIEFING ROOM ISSUES the ADMINISTRATION

Home • Briefing Room • Statements & Releases

The White House
Office of the Press Secretary

E-Mail Tweet Share +

For Immediate Release

February 12, 2013

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

Statewide Program Updates

- Policy & Program Improvement
- Project Update - Incident Reporting Automation
- General Reminders
- Project Update - Emergency Function (EF) 18, Cyber Security Annex

Policy and Program Improvement

TABLE OF CONTENTS

- **5300 INTRODUCTION**
- **5305 INFORMATION SECURITY PROGRAM MANAGEMENT**
- **5315 SECURE SYSTEM ENGINEERING**
- **5330 INFORMATION SECURITY AND PRIVACY TRAINING AND AWARENESS**
- **5340 BUSINESS CONTINUITY**
- **5345 INFORMATION SECURITY COMPLIANCE**
- **5350 INFORMATION SECURITY MONITORING**
- **5355 INFORMATION SECURITY INCIDENT RESPONSE AND FORENSICS**
- **5360 RISK MANAGEMENT**
- **5365 OPERATIONAL SECURITY**
- **5370 ENDPOINT DEFENSE**
- **5375 IDENTITY AND ACCESS MANAGEMENT**
- **5385 PHYSICAL SECURITY**
- **5390 PRIVACY**

Policy and Program Improvement

5305.1 INFORMATION SECURITY OFFICER

(Revised XX/XX)

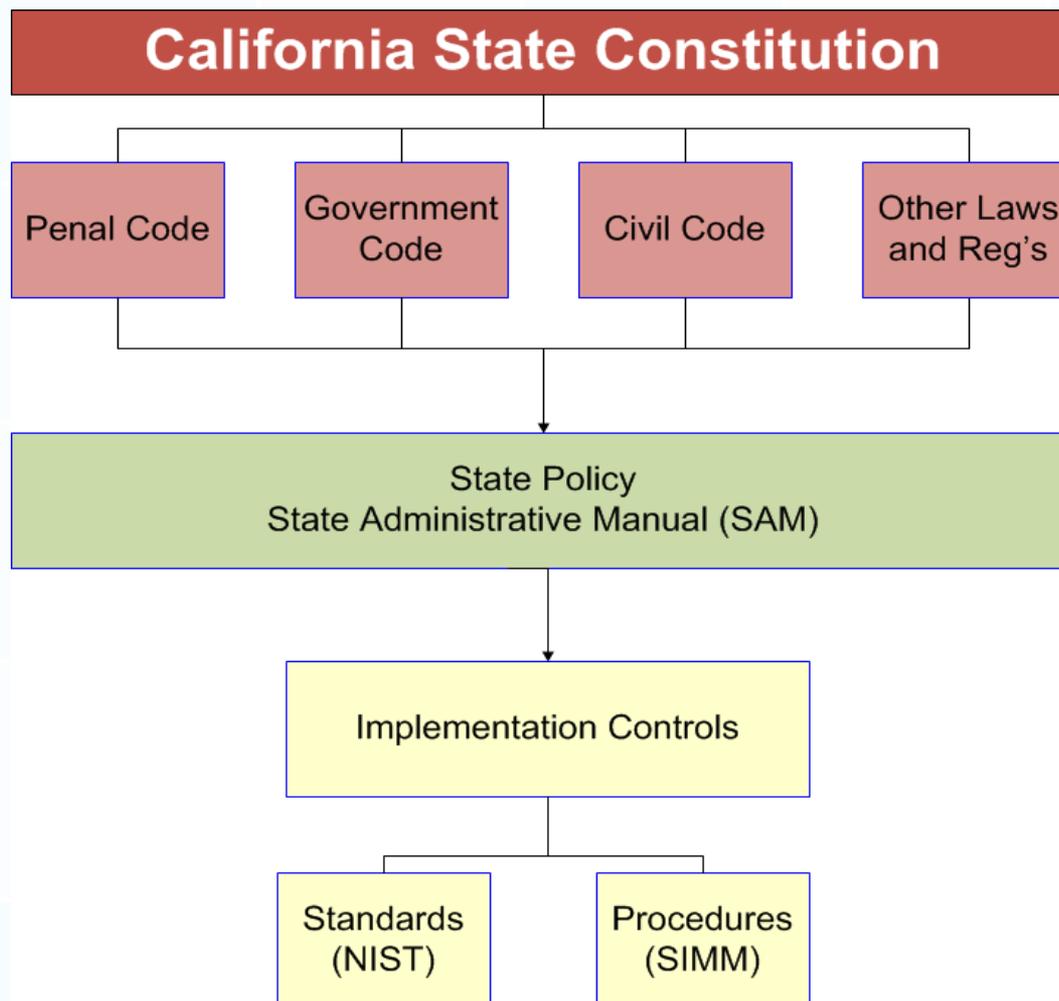
Policy: Each entity is required to appoint an Information Security Officer (ISO) with management and oversight responsibility for the entity's Information Security Program.

Background: The ISO must possess the training, skills, and knowledge sufficient to execute the program requirements. Within the first 6 months of appointment, the ISO shall complete the "ISO Basic Training" course offered by the State's Office of Information Security.

The Director of the Office of Information Security shall coordinate the activities of agency information security officers, for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards.

Implementation Controls: SIMM-XX; NIST PM-2

Policy and Program Improvement



Incident Reporting Automation

- **Development Phase – In Progress**
- **Implementation Phase – October 2013**

Reminders

■ FOUO/TLP Reminder

■ Follow Sensitive Information Handling Instructions

- For Official Use Only (FOUO)
- Traffic Light Protocol (TLP)

■ DON'T:

- Post or make available on a public website
- Provide to the media

■ DO:

- Limit distribution to protect information assets

Reminders

■ Traffic Light Protocol:

Red	Amber	Green	White
<p>Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</p>	<p>Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.</p>	<p>Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.</p>	<p>TLP: WHITE information may be distributed without restriction, subject to copyright controls.</p>

■ Additional information on TLP:

<http://www.us-cert.gov/contact/tlp.html>

Reminders

- Meeting registration is requested to:
 - Accurately account for the number of hand-outs / materials
 - Track attendance/participation
- Next meeting is July 11, 2013

State Emergency Plan
Emergency Function 18
Cyber Security Annex

Technology Agency
Office of Information Security

Enterprise Architecture

Technology Agency Enterprise Architecture

Closing

**Thank you for joining us and
all that you do!**