California Technology Agency
Office of Information Security

Information Security Officer Meeting

January 12, 2011

Meeting Agenda

California Technology Agency
Office of Information Security

-----Topics-----	
Opening Remarks Keith Parker, Acting Director and Chief Information Security Officer	5 minutes
Office of Technology Services, Secure Internet Gateway (SIG) Marc Hanson, OTech Security Management Division	60 minutes
Cyber Storm III After Action Report Marianne Chick, Information Security Manager	30 minutes
Short Subjects: ☑ Policy Update ☑ Legislative Update ☑ Required Training ☑ Security Compliance Reporting	20 minutes
Q&A and Closing	5 minutes

CyberStorm III

The Office of Information Security (OIS), in cooperation with the California Emergency Management Agency (CalEMA) , participated as a “full player” in international Cyber Storm III exercise activities that took place in September 2010. One of the goals of this exercise was to identify DHS’s role in its evolving National Cyber Incident Response Plan (NCIRP), and how to link state plans to the National plan.

California’s objectives were to determine how to better coordinate with the Federal and local governments, other States, communities, and private partners, all the while testing the effectiveness of our own State plans and procedures related to cyber events.

Several “injects” developed by individual participating agencies, counties, cities and the CyberStorm IT/Comms community were unleashed on California state government’s critical technical infrastructure. These injects included multiple infected hosts, phishing, website defacements, extortion, compromised DNS records, redirections to hacker sites, botnets, all ca.gov websites and OTech hosted email were inoperable.

Policy Updates

California Technology Agency
Office of Information Security

- SAM/SIMM Updates:
  - Smartphone *(ITPL 10-19, issued 12/30/2010)*
  - Privacy *(in development)*
  - Required Security Reporting *(SIMM Forms Updated, Forum held on 1/07/2011)*
  - ISO Roles and Responsibilities Guide Update to include qualification criteria for ISOs (*in development*)

Legislative Update

California Technology Agency
Office of Information Security

AB 2091	PRA Exemption	Approved by the Governor & Chaptered 8/27/2010
AB 2408	OCIO - California Technology Agency	Approved by the Governor & Chaptered 9/28/2010
SB 1055	OCIO Fingerprint	Approved by the Governor & Chaptered 9/24/2010

Legislative Update – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

AB 2408

- Governor's Reorganization Plan clean-up bill
- Codifies Executive Order S-10-03
- Name change – OCIO to California Technology Agency
- Extends the OCIO's sunset set date from 2013 to 2015
- Imposes additional duties on the Secretary of the California Technology Agency.
- Strengthens the OIS's oversight and enforcement authority.

Legislative Update – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

AB 2091

- Public Records Act (PRA) exemption.
- Information Security records that would reveal vulnerabilities or would increase the potential for an attack on an information system.
- Although AB 2091 does limit the public's right of access, it is a very limited and targeted exemption.

Legislative Update – *Continued*

California Technology Agency
Office of Information Security

SB 1055

- Technology Agency - fingerprints and criminal history checks.
- Technology Agency employees and contractors that have access to sensitive or confidential information.
- Conviction of crimes related to dishonesty, fraud, or deceit and is substantially related to the duties of the person.
- There is an appeals process.

Required Training for Designees – 2011 Sessions

California TECHNOLOGY AGENCY
Office of Information Security

- ISO Basic Training
  - February 16, 2011
  - June 8, 2011
  - September 13, 2011 and
  - December 9, 2011

- Basic Privacy Coordinator Training
  - January 20, 2011

Other Tidbits

California TECHNOLOGY AGENCY
Office of Information Security

- **Grant Application**
  - 9 Security-related grant projects included in application
  - Just over $7.5 million
  - Applications under review by CalEMA award committee
  - Awaiting award announcement
- **DHS PSA Challenge**

DHS PSA Challenge

California Technology Agency
Office of Information Security

Stop. Think. Connect. PSA Challenge:

- DHS challenge kicked-off November 8, 2010
- Looking for videos that:
  - will educate Americans about Internet safety.
  - inspire Americans to **Stop. Think. Connect.**

Challenge Deadline:

Monday, February 14, 2011, at 11:59 p.m. ET.

DHS PSA Challenge – *Continued*

California Technology Agency
Office of Information Security

Categories:

PSAs directed towards any of the following audiences:

- Teenagers (13-17)
- Young Adults (18-24)
- Parents of Teenagers
- Older Americans

More information about how to participate:

http://www.dhs.gov/files/events/stop-think-connect-psa challenge.shtm

Security Reporting 2011

California TECHNOLOGY AGENCY
Office of Information Security

All SIMM forms except the Agency Information Security Incident Report have been updated. Agency's are to use the updated versions for Jan 2011.

Report/Activity	Policy Section	Instructions and Forms	Due Date
Agency Designation Letter	5360.1	SIMM 70A	Annually by January 31 and within ten (10) business days of any change in designee
Agency Risk Management and Privacy Program Compliance Certification	5360.1	SIMM 70C	Annually by January 31
Disaster Recovery Plan (Complete)	5360.1	SIMM 65A SIMM 70D	Annually pursuant to the DRP Submission Schedule
Disaster Recovery Plan Certification (No-Change)	5360.1	SIMM 70B	Every-other year pursuant to the DRP Submission Schedule in lieu of a complete plan when no changes have occurred since last submission.
Agency Information Security Incident Report	5360.1	SIMM 65B SIMM 65C SIMM 65D	Within ten (10) business days from the date of notification to CHP's Emergency Notification and Tactical Alert Center (ENTAC)
Agency Telework and Remote Access Security Compliance Certification	5340	SIMM 70E	Initial by July 1, 2010. Annually by January 31 thereafter, commencing January 31, 2011.

Security Reporting 2011 – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

- **Purpose** of reporting is to ensure agency
  - Understands its responsibility for security
  - Is aware of and is appropriately managing risk
  - Implementing timely and appropriate corrective actions
  - Achieving regulatory and policy compliance
  - To ensure the trust of Californians by protecting the State's information assets.

- It's NOT just about filling in or checking the boxes!

Security Reporting 2011 – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

- **Benefits of participation**
  - Promotes the entity's recognition and support for the state's need to understand its security poster across all state entities.
  - Entity will receive credit for participation through scorecard.
  - Entity receives other benefits. For example, DL provisions for critical alert and emergency notifications.

Security Reporting 2011 – *Continued*

California Technology Agency
Office of Information Security

- **Expectations**
  - All agencies subject to compliance with state policy and standards, and Government Code Sections 11546.1 and 11549 et.seq. will participate.
  - Others are strongly encouraged to voluntarily participate.

Security Reporting 2011 – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

Where to Access Current Forms ?

http://www.cio.ca.gov/OIS/Government/policy.asp

Security Reporting 2011 – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

Schedule of Required Reporting Activities

The following provides a summary schedule of required reporting activities with corresponding due dates. Unless otherwise nc
of Information Security.

Report/Activity	Policy Section	Instructions and Forms	Due Date
Agency Designation Letter	5360.1	SIMM 70A	Annually by January 31 and within ten (10) business days of any change in designee
Agency Risk Management and Privacy Program Compliance Certification	5360.1	SIMM 70C	Annually by January 31
Disaster Recovery Plan (Complete)	5360.1	SIMM 65A SIMM 70D	Annually pursuant to the DRP Submission Schedule
Disaster Recovery Plan Certification (No-Change)	5360.1	SIMM 70B	Every-other year pursuant to the DRP Submission Schedule in lieu of a complete plan when no changes have occurred since last submission.
Agency Information Security Incident Report	5360.1	SIMM 65B SIMM 65C SIMM 65D	Within ten (10) business days from the date of notification to CHP's Emergency Notification and Tactical Alert Center (ENTAC)
Agency Telework and Remote Access Security Compliance Certification	5340	SIMM 70E	Initial by July 1, 2010. Annually by January 31 thereafter, commencing January 31, 2011.

Security Reporting Scorecard

California Technology Agency
Office of Information Security

- **Initial Scorecards Based On:**
  - Four required submissions
  - Receipt only
- **Later Scorecards Will Include:**
  - Voluntary participation
- **May Include:**
  - Completeness of submissions
  - Timeliness of submissions
  - Incident reporting in aggregate

Security Reporting Score Card – *Continued*

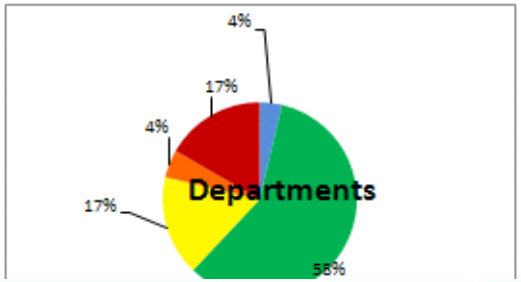
California Technology Agency
Office of Information Security

Agency Security Filing Compliance - November 2010

Agency	Compliant	In Progress	No Progress	Filing Progress
BTH	11	2	1	86%
CDCR	1	1	1	50%
EPA	5	1	0	92%
HHS	14	1	0	97%
LWDA	5	1	1	79%
Resources	7	11	8	48%
SCSA	8	4	0	83%
Other	16	2	7	68%
State Total	67	23	18	73%

Scorecard	Departments
Blue	4
Green	63
Yellow	18
Orange	5
Red	18

Scorecard Status Key
BLUE - Compliant - All filings received and fully accepted.
GREEN - Compliant - All filings received and are pending OIS review.
YELLOW - At Risk - One filing not received.
ORANGE - At Risk - Two or three filings not received.
RED - No filings received.



Sample

Security Reporting Score Card – *Continued*

California TECHNOLOGY AGENCY
Office of Information Security

Legend

Red	No Progress
Orange	At risk - two or three items missing.
Yellow	At risk - one item missing.
Green	Compliant - All filings received and are pending OIS review.
Blue	Compliant - All filings received and fully accepted.

Questions

Closing

California Technology Agency
Office of Information Security

- Feedback
  - New method for meeting evaluations.
  - You will receive an email with a link to a Zoomerang survey.
  - We appreciate your feedback.
- Next Meeting
  - March 10, 2011
  - Special Guest State Threat Assessment Center