



California
TECHNOLOGY AGENCY
Office of Information Security

Information Security Officer Meeting

November 10, 2011

Meeting Agenda

----- Topics -----	
<u>Opening Remarks</u>	5 minutes
<u>Statewide Security Program Updates</u>	40 minutes
<u>California Highway Patrol, Computer Crimes Investigations Unit</u> Sgt. Kelly Dixon	20 minutes
<u>Open Discussion</u>	40 minutes
<u>Q&A and Closing</u>	15 minutes

Opening Remarks

- **Welcome**
- **AIO/AISO Meetings**



Keith Tresh, Director and CISO

Organizational Update

- **OTech Security Management Division was merged into the OTech Operations Division, and are now called “Security Management Service”.**
- **OIS Vacancy Status:**
 - **RA scheduled to start 11/14/2011**

Legislative Update

- **SB 24 (Simitian)**
 - Approved by Governor August 31, 2011
 - Effective January 2012
 - Requires more specific language in breach notifications
 - Requires an electronic copy of breach notification be provided to AG for a single incident involving 500+ individuals
- **Chaptered legislation available at:**
www.leginfo.ca.gov

Legislative Update (*Continued*)

- **SB 24 Recommended Actions**
 - Continue to follow OIS SIMM 65D procedures
 - Review adopted legislation
 - Consult with legal counsel
- **Chaptered legislation available at:**
www.leginfo.ca.gov

Policy Updates

- Tech Agency conducting review of policies
- Policy and Standards Refresh
 - OIS completed a policy gap analysis
 - Effort identified the need for:
 - 14 Policy Updates
 - Development of 19 Standards and 4 Procedures
 - Intend to leverage the gap analysis recommendations in forward movement

Policy Updates (*Continued*)

■ SAM/SIMM Updates

■ ISO Roles and Responsibilities Guide Update (discussions with HR complete) to include:

- Specific ISO position *core competency* criteria for ISOs and appointing power checklist
- Appointing power certification that AISO/ISO appointments meet the criteria.

■ Privacy (still in development) to include:

- Statement and Notices Standard
- Individual Access Standard
- Privacy Impact Assessment Standard

Status on Required Security Reporting Activities

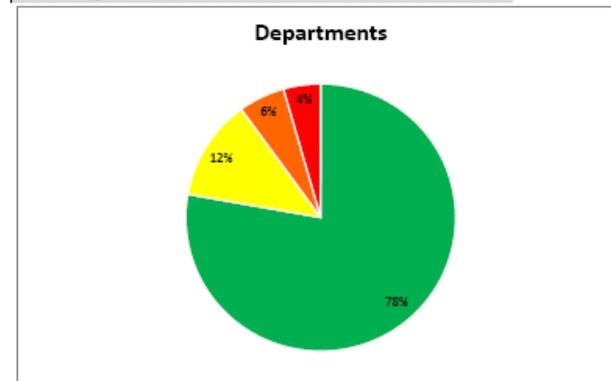
- Name change reflected 8/31
- 84% Overall
 - 2% Decrease from May 2011
 - Missing 7/15 DRP filings
- Next publication November 2011

Status of Required Security Reporting Activities

Agency	Compliant	In Progress	No Progress	Progress
BTH	13	1	0	96%
CDCR	2	1	0	83%
EPA	5	1	0	92%
HHS	12	3	0	90%
LWDA	4	3	0	79%
Resources	10	0	0	100%
SCSA	11	0	1	92%
Other	13	7	3	72%
State Total	70	16	4	87%

Status	Departments
Green	70
Yellow	11
Orange	5
Red	4

Status Key
GREEN - Compliant - All filings received.
YELLOW - At Risk - One filing not received.
ORANGE - At Risk - Two or three filings not received.
RED - No filings received.



Status of Required Security Reporting Activities - August 2011

Required Security Reporting Activities *(Continued)*

- **Purpose of reporting is to ensure the *agency and the agency head***
 - Understand 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!**

Required Security Reporting Activities *(Continued)*

- **Purpose of reporting is also to enable *Technology Agency* to:**
 - Understand statewide security and risk posture
 - Establish security metrics for identifying:
 - Statewide issues and trends
 - Program gaps and needs

National Cyber Security Awareness Month

- All Governor's issued Proclamation or Letter of Support
- Cyber pledge – Ranked in the top ten
 - 5th among states (overall number of pledges)
 - 4th among local governments (Sacramento)
- Distributed awareness material and helped others launch their events
- California is now a *Stop.Think.Connect* campaign coalition member

IT Security Awareness Fair

- Attended by over 400 government employees this year!
- Many thanks to our public sector Advisory Board Members for:
 - Working within the short timeframe
 - Identifying relevant content
 - Getting people to the event

2011 ITSAF

Advisory Board Members

- Carl Gunderson, CalEPA
- Carla Zuehlke, OSI
- Christian Turner, EDD and LWDA
- Denise Mellor, FTB and SCSA
- Glen Carson, Resources
- Helen Woodman, DOF
- Scott MacDonald, CDCR
- Stephanie Cervantes, CalPERS
- Steve Moore, DHCS
- Thys Bohr, DVA
- Vitaliy Panych, EDD

ITSAF Follow-up Content

■ Topic: Security Metrics

- Is there interest in a presentation on this topic?
- December or January?

■ Topic: Risk Assessment

- Is there interest in a workshop or presentation on this topic?
- Are you willing to take a short survey to in advance of the workshop to optimize your learning?

Training Resources

- **Next ISO Basic Training Class**
 - **December 9, 2011 (Class is full)**
- **Free Online Training:**
 - **DHS/FEMA State Cyber Security Training**
<http://www.teex.com/teex.cfm?pageid=agency&area=OGT&templateid=1810>
 - **DoD Assurance Awareness Training**
<http://iase.disa.mil/eta/online-catalog.html#iaatraining>
- **MS-ISAC/SANS 2012 Aggregate Buy**
<http://msisac.cisecurity.org/resources/videos/sans-training.cfm>

Free Awareness Resources

■ National Webcast Initiative

- Next Webcast: Thursday, December 15, 2011
- Topic: *Social Networking -The Latest Security Issues and How to Manage Them*

<http://msisac.cisecurity.org/webcast/>

■ Free Tools and Resources:

- National Cyber Security Alliance

<http://staysafeonline.org/tools-resources>

Statewide Program Update

- **Incident Management**
 - **Automation of Incident Reporting Process**
 - Procurement Phase Completed by 12/2011
 - DGS Preparing to Issue Notice of Intent to Award
 - **Status of SIMM 65C Reviews**
 - Make sure they are complete
 - Many lack
 - reference to OIS tracking number
 - identification of root cause of incident
 - Corrective action that addresses root cause

Statewide Program Updates (Continued)

■ Risk Management

- DNS Security
- Enterprise Risk Management
 - Unified Framework and Tool
 - Requires resources and extension on the grant performance period to move forward
- Critical Alerts and Advisories

Statewide Program Updates (Continued)

■ Federal Initiatives

- **DHS Nationwide Cyber Security Review**
 - 71 question survey
 - Conducted via the US-CERT portal
 - Conducted October 1 through November 15
 - Scope of effort is all 50 states CIO, CISO and IT staff at Human Services, Tax & Revenue, and Transportation organizations.
- **Reminder – Submissions are due Nov. 15**

Statewide Program Updates (Continued)

■ Latest NIST News:

- National Initiative on Cybersecurity Education (NICE) Issues Cybersecurity Workforce Framework for Public Comment
- Draft Roadmap for Cloud Computing Technology

Statewide Program Updates (Continued)

■ Latest NASCIO Publications:

- **The Heart of the Matter: A Core Services Taxonomy for State IT Security Programs**
- **State CIO Top Ten Policy and Technology Priorities for 2012**

<http://www.nascio.org/>

Friendly Reminders

Reminder ISO Meeting Changes:

- **Registration is required so that we may:**
 - **More accurately account for the number of hand-outs /materials.**
 - **More easily track attendance/participation.**
- **A link will be sent to CIOs and ISO/ISO back-ups on designee list.**
- **CIOs/ISOs may forward to others**

Friendly Reminders (*Continued*)

- **Follow FOUO Sensitive Information Handling Instructions**
 - **DON'T:**
 - **Post or make available on a public website**
 - **Provide to the media**
 - **DO:**
 - **Limit distribution and sharing to those that have a need to act on the information to protect information assets**

California Highway Patrol Computer Crimes Investigations Unit

Sergeant Kelly Dixon

CCIU Discussion Topics

1. Customer Service
2. Wireless Access Points

Risk Mitigation Strategies:

- **WAP Policy – Free Template at SANS.org**
<http://www.sans.org/security-resources/policies/>
- **Secure Configurations – See guidance at:**
US-CERT http://www.us-cert.gov/reading_room/Wireless-Security.pdf
OIS <http://www.cio.ca.gov/OIS/Government/library/awareness.asp#tips>

Open Discussion

Closing

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

**The meeting evaluation survey. Will be
emailed to you. Please complete as your
feedback is important to us!**