



California
TECHNOLOGY AGENCY
Office of Information Security

Information Security Officer Meeting

July 14, 2011

Meeting Agenda

----- Topics -----	
<u>Opening Remarks</u>	5 minutes
<u>Short Subjects:</u> <input checked="" type="checkbox"/> Organization Update <input checked="" type="checkbox"/> Policy Update <input checked="" type="checkbox"/> Required Training <input checked="" type="checkbox"/> Statewide Security Program Updates	40 minutes
<u>Incident Reporting and Criminal Investigations - OIS and California Highway Patrol (CHP)</u> Officers Ryan Duplissey and Pete Lockhart, Computer Crimes Investigations Unit	30 minutes
<u>Recent Incident and Lessons Learned - California State Lottery</u> Mary Morshed, Information Security Officer	30 minutes
<u>New State CIO and Agency Secretary Introduction</u> Carlos Ramos, California Technology Agency	10 minutes
<u>Q&A and Closing</u>	5 minutes

Thanks for joining us!

Recent Organizational Changes

- **New Agency Secretary**
 - Carlos Ramos
- **OIS Vacancies (3/8):**
 - Director/CISO
 - Statewide Incident Management Program Manager (vacancy effective 8/2010)
 - Statewide Risk Management Program Manager (vacancy 8/2011)

Statewide Security Program

■ Statutory functions

- What is OIS required to do (GC 11549)?
 - Policy, Standards, Guidelines, Procedures
 - Educate, train and raise awareness
 - Collect, track and report on security incidents
 - Ensure development, maintenance, testing and filing of disaster recovery plans
 - Represent CA before federal, state and local government entities, and private industry
 - Track and report on agency compliance

Continuous Process Evaluation & Improvement Objectives

- Evaluate OIS processes and forms
- Explore/implement alternatives that:
 - Simplify processes
 - Reduce impact to agencies/departments
 - Achieve greater security compliance
 - Meet OIS statutory responsibilities
- We need your continued feedback and help!

Policy Updates

- **SAM/SIMM Updates**
 - **ISO Roles and Responsibilities Guide Update (still in discussions with HR) to include:**
 - Specific ISO position qualification 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

Security Compliance Reporting

- Name change
- % Increase from February
- Next publication August 2011

Agency Security Filing Compliance - February 2011

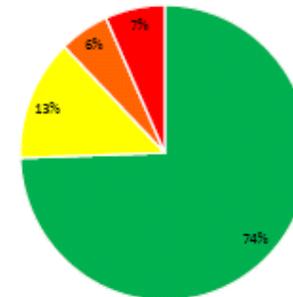
Agency	Compliant	In Progress	No Progress	Filing Progress
BTH	13	1	0	96%
CDCR	1	2	0	67%
EPA	5	1	0	92%
HHS	13	2	0	93%
LWDA	4	3	0	79%
Resources	9	1	0	95%
SCSA	8	3	1	79%
Other	14	4	3	70%
State Total	67	17	6	84%

Scorecard	Departments
Green	67
Yellow	12
Orange	5
Red	6

Scorecard 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.

Departments



Security Compliance Reporting

(Continued)

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

Required Training for Designees

- **ISO Basic Training:**
 - September 13, 2011
 - December 9, 2011
- **Basic Privacy Coordinator Training**
 - Developing alternative delivery option.
- **Basic DR Coordinator Training**
 - Curriculum under development

Statewide Program Updates

- **Disaster Recovery Management**
 - 7/20 DR Coordinator Meeting Canceled
 - Status of DR Plan Reviews
 - Emergency Function #18, Cyber Security
 - Requires resources and an Enterprise BIA
 - Target for Initial Draft – December 2012

Statewide Program Updates (Continued)

- **Incident Management**
 - **California Cyber Incident Response Plan**
 - Continuation of CalEMA Good Harbor project
 - Will reside within:
 - State Emergency Plan (SEP) EF#18 Cyber Security
 - Target for revised draft - December 2012
 - **Automation of Incident Reporting Process**
 - RFP released 12/15/10; 34 letters of bid intent
 - Draft proposals due **TODAY**; Finals 9/9/11

Statewide Program Updates (Continued)

- **Risk Management (continued)**
 - Security Awareness and Privacy Training
 - DNS Security
 - Pilot 6/27 thru 10/7/2011
 - Implementation 10/8 thru 12/30/2011
 - Enterprise Risk Management
 - Unified Framework and Tool
 - Requires resources and extension on the grant performance period to move forward

Statewide Program Updates (Continued)

- **Relationship and Trust Management**
 - **Multi-jurisdictional Interactions**
 - **Federal * State * Local * Tribal * Private**
 - **Information Sharing**
 - **FOUO – What’s it mean? What are the handling caveats?**

Statewide Program Updates (Continued)

- **2010 Grant Application**
 - 9 Security-related grant projects included in application
 - Just over \$7.5 million
 - **2010 Award = \$250K**

Statewide Program Updates (Continued)

Reminder ISO Meeting Changes:

- Registration will be 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

Incident Reporting and Criminal Investigations

Partnering with Law Enforcement

Incident Reporting

- Follow the State's prescribed process:
 - Immediate reporting to **(916) 843-4199**
 - 24/7 Centralized Intake via CHP ENTAC
 - Alerts are generated to CHP CCIU and OIS
 - 2-4 hour response-*regular business hours*
- Indicate **URGENT** response needed for reports made outside normal business when needed.
- Limit activities which may damage or destroy evidence.

Criminal Investigations

- **For incidents involving criminal activity:**
 - The State agency is the victim of a crime.
 - Law Enforcement (LE) is your partner.
 - LE (CHP) has jurisdiction over criminal investigations involving crime against state agencies.
 - They are our LE partner and need evidence to build a case for prosecution.

Assisting Law Enforcement

- Limit activities which may damage or destroy evidence until consulted by the CCIU Officer.
- CCIU will instruct/guide agency on what and how evidence is to be collected.
- Order of Preferred Method:
 - CCIU Officer collects
 - CCIU contacts another LE partner to collect
 - CCIU guides/relies on agency personnel

Consequences of Not Limiting Activities Until Consulted by LE

- Potential evidence is damaged or destroyed.
- LE unable to pursue criminal case.
- Criminals free to continue illegal activity.
- Agency, State and other possible victims unable to recover monetary loss/compensation.
- This would be reflected in the follow-up written Security Incident report.

Recent Incident and Lessons Learned

Mary Morshed, ISO
California State Lottery

New State CIO and Agency Secretary Introduction

Carlos Ramos

California Technology Agency

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!**