



California
TECHNOLOGY AGENCY
Office of Information Security

Information Security Officer Meeting

September 8, 2011

Meeting Agenda

----- Topics -----	
<u>Opening Remarks</u>	5 minutes
<u>New Director/State CISO Introduction: Keith Tresh</u>	10 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>California Highway Patrol, Computer Crimes Investigations Unit</u> Sgt. Kelly Dixon	30 minutes
<u>California Technology Agency, Office of Technology Services, CES Project</u> Kermit Bonner, Security Management Division	30 minutes
<u>Q&A and Closing</u>	5 minutes

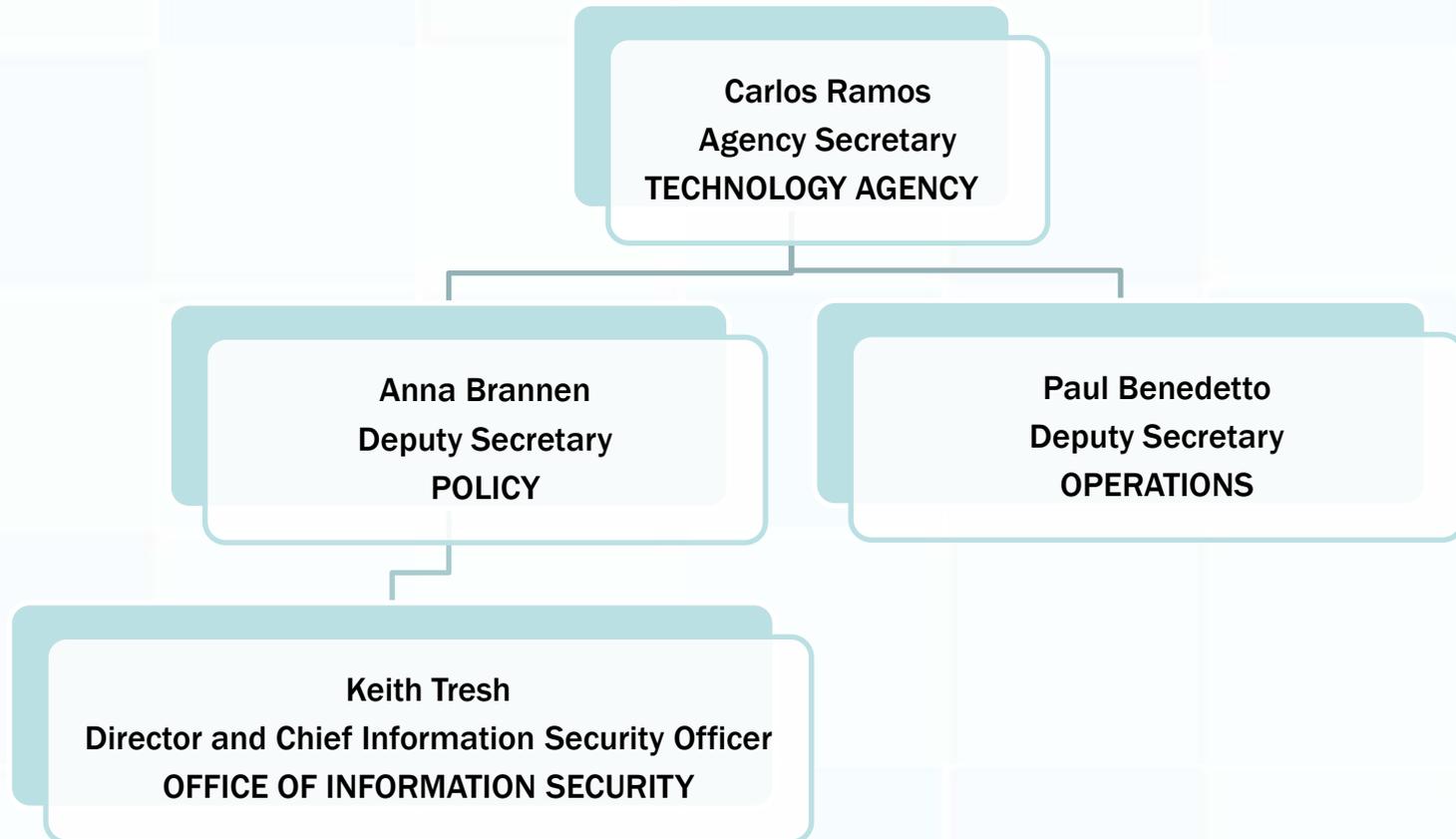
Thanks for joining us!

New OIS Director/State CISO Introduction

Keith Tresh

Organizational Update

■ Technology Organizational Structure



Organizational Update (*Continued*)

- **OIS Vacancies (2):**
 - **Statewide Incident Management Program Manager (vacancy effective 8/2010)**
 - **Statewide Risk Management Program Manager (vacancy 8/2011)**

Statewide Security Program Priorities

- **Identify vulnerable systems**
- **Refresh Security Policy and Standards**
 - Intend to leverage the gap analysis recommendations in forward movement
- **Establish/expand ISO Advisory Group Activities**
 - Increase information sharing
 - Leverage the capability/good ideas of others
- **Education and Awareness**

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

Policy Updates

- **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

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

Status on Required Security Reporting Activities

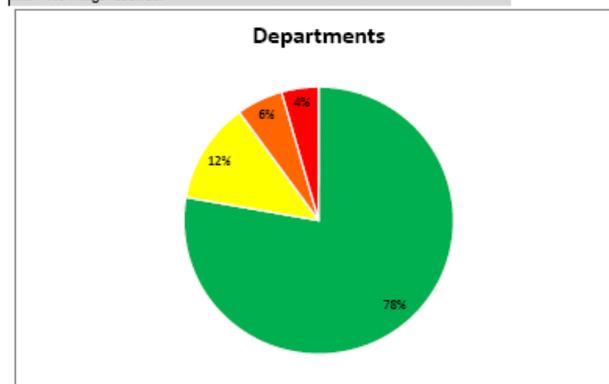
- Name change reflected 8/31
- 84% Overall
 - 2% Decrease from May 2011
 - Missing 7/15 DRP filings
- Next publication November 2011

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 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**
 - Next DR Coordinator Meeting 10/19
 - Status of DR Plan Reviews
 - Emergency Function #18, Cyber Security
 - Requires resources and an Enterprise BIA
 - Target for Initial Draft – June 2012

Statewide Program Updates (Continued)

- **Incident Management**
 - **California Cyber Incident Response Plan**
 - Continuation of Cal EMA Good Harbor project
 - Will reside within:
 - State Emergency Plan (SEP) EF#18 Cyber Security
 - Target for revised draft - June 2012
 - **Automation of Incident Reporting Process**
 - RFP released 12/15/10; 34 letters of bid intent
 - Final Proposals Due 9/9/11

Statewide Program Updates (Continued)

■ Risk Management

■ Security Awareness

■ National Cyber Security Awareness Month (NCSAM) Initiatives

- Letter to Governor's for Proclamation
- MS-ISAC Awareness Month Toolkit
- Cyber Pledge Contest 9/1 to 10/31

URL: www.ms-isac.org

■ OIS Supporting Initiatives

- Pay Warrant Message
- Governor's Proclamation
- Distribution of Posters, Calendars, Awareness Materials

Statewide Program Updates (Continued)

■ Risk Management (*continued*)

■ 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

■ Critical Alerts and Advisories

Statewide Program Updates (Continued)

■ 2010 HSGP Grant Application

- 9 Security-related grant projects included in application
- Just over \$7.5 million
- **2010 Award = \$250K**
- **2011 HSGP Grant Applications Due October 1, 2011**
- Additional cyber grant guidance from DHS

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.
- **MS-ISAC Member and Non-Member Services**

Soliciting Input

- **Are ISOs interested in Vendor Forums ?**
 - **Facilitated product neutral presentations**
 - **Security problem/topic specific**
- **If so, what is the preferred frequency?**

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. Copyright Infringement / Unauth P2P cases (music/movies, etc.)**
- 2. Criminal versus Administrative Investigations**
- 3. Request for clarity when reporting incidents**

California Email Service (CES)

Kermit Bonner

Office of Technology Services

Security Management Division

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!**