



California  
**TECHNOLOGY AGENCY**  
Office of Information Security

# Information Security Officer Meeting

March 10, 2011

# Meeting Agenda

----- Topics -----	
<u><b>Opening Remarks</b></u> Keith Parker, Acting Director and Chief Information Security Officer	5 minutes
<u><b>California Highway Patrol, State Threat Assessment Center (STAC)</b></u> Lieutenant Ryan Stonebraker	60 minutes
<u><b>Short Subjects:</b></u> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Policy Update</li> <li><input checked="" type="checkbox"/> Legislative Update</li> <li><input checked="" type="checkbox"/> Required Training</li> <li><input checked="" type="checkbox"/> Security Compliance Reporting</li> </ul>	20 minutes
<u><b>Other Statewide Program Updates</b></u>	30 Minutes
<u><b>Q&amp;A and Closing</b></u>	5 minutes

# Program Impact Due to Continued Resource Limitations

## ■ Mandated 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
- Report on Agency Compliance

### ■ What *can* OIS do given its current resources?

# Policy Updates

- **SAM/SIMM Updates**
  - **ISO Roles and Responsibilities Guide Update (still in development) to include:**
    - Minimum qualification (MQ) criteria for ISOs and appointing power checklist
    - Appointing power certification that AISO/ISO appointments meet the MQ criteria.
  - **Privacy (still in development) to include:**
    - Statement and Notices Standard
    - Individual Access Standard
    - Privacy Impact Assessment Standard

# Legislative Update

- Over 2K pieces of CA legislation introduced
- Watching:
  - Federal
    - The Cybersecurity Enhancement Act
    - Protecting Cyberspace as a National Asset Act
    - The Grid Reliability and Infrastructure Defense (“GRID”) Act
  - State
    - SB24 - Breach Notification
    - SB102 - Telecommunications/Geotagging
    - SB242 - Social Networking Privacy Act
    - AB 452 - Electronic tracking devices

# Required Training for Designees

- **ISO Basic Training:**
  - June 8, 2011
  - September 13, 2011
  - December 9, 2011
- **Basic Privacy Coordinator Training**
  - Scheduling of additional sessions in progress
- **Basic DR Coordinator Training**
  - Curriculum under development
  - First delivery target 7/2011

# Required Training for Designees (Continued)

## Who is attending?

- **ISO Basic Training:**
  - Total Attendees 124 Total Designees 76
  - 61% were Designees
- **Basic Privacy Coordinator Training**
  - Total Attendees 117 Total Designees 48
  - 41% were Designees
- **100% course satisfaction rating**

# Security Compliance Reporting

- **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!**

# Security Compliance Reporting (Continued)

- Scorecard
- Four required compliance documents.
  - 70A, 70C, 70E and DR Plan
- Updated legend
  - Blue was removed

Agency Security Filing Compliance - February 2011

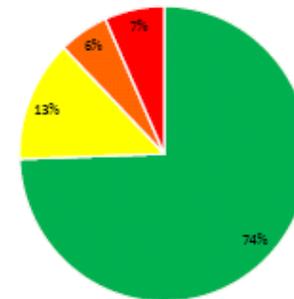
Agency	Compliant	In Progress	No Progress	Filing Progress
BTH	13	1	0	96%
CDCR	1	2	0	67%
EPA	5	1	0	92%
HHS	13	2	0	93%
LWDA	4	3	0	79%
Resources	9	1	0	95%
SCSA	8	3	1	79%
Other	14	4	5	70%
State Total	67	17	6	84%

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)

## Security Scorecard Legend

**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.

# Security Compliance Reporting (Continued)

- **Make sure...**
  - the entity head and CIO are aware of the security reporting scorecard publication.
  - the Agency CIO and Agency ISO are aware of any problems you are having with completing the forms for your entity.

# Statewide Program Updates

- **Disaster Recovery Management**
  - DR Plan Reviews (what we look for and why)
  - Emergency Function #18, Cybersecurity
- **Incident Management**
  - California Cyber Incident Response Plan
  - Automation of Incident Reporting Process
- **Risk Management**
  - DNS Security
  - Enterprise Risk Management
    - Unified Framework and Tool

# Statewide Program Updates (Continued)

- **Risk Management (continued)**
  - Security Awareness and Privacy Training
  - Telework, Remote Access and Smartphones
- **Relationship and Trust Management**
  - Multi-jurisdictional Interactions
    - Federal \* State \* Local \* Tribal \* Private
    - Information Sharing

# Statewide Program Updates (Continued)

- **Disaster Recovery Management**
  - **DR Plan Reviews**
    - What We Look For
    - Why It Matters
  - **Emergency Function #18, Cybersecurity**
    - Announced at January SWEPC Meeting
    - Kickoff Meeting w/CalEMA February 24, 2011
    - Requires resources and an Enterprise BIA
    - Draft due December 2011

# 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

- Revised draft due December 2011

### ■ Automation of Incident Reporting Process

- RFP released 12/15/10; 34 letters of bid intent

- Draft proposals due 4/22/11; Finals 6/10/11

# Statewide Program Updates (Continued)

## ■ Risk Management

### ■ DNS Security

■ Pilot 6/2011

■ Implementation 12/2011

## Enterprise Risk Management

### ■ Unified Framework and Tool

■ Framework SOW under review

■ Anticipate release of the framework bid by 5/2011.

# Statewide Program Updates (Continued)

## ■ Risk Management (*continued*)

- Security Awareness and Privacy Training
  - How many do not have a training program today?
  - How many have a program in place today which costs \$2 or less per individual seat?
- Telework, Remote Access and Smartphones
  - Implementation questions?

# Statewide Program Updates (Continued)

## ■ 2010 Grant Application

- 9 Security-related grant projects included in application
- Just over \$7.5 million
- Applications under review by CalEMA award committee
- Still awaiting award announcement

# Statewide Program Updates (Continued)

## 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

# Closing

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

**Please complete the meeting  
evaluation survey.**

**Your feedback is important to us!**