



California
TECHNOLOGY AGENCY
Office of Information Security

Statewide Disaster Recovery Coordinator Meeting

January 18, 2012

Meeting Agenda

| ----- Topics ----- | |
|--|------------|
| <u>Opening Remarks</u> | 5 minutes |
| <u>Short Subjects:</u> <input checked="" type="checkbox"/> Organization Update <input checked="" type="checkbox"/> Statewide Disaster Recovery Program Update | 30 minutes |
| <u>California State Emergency Plan Emergency Functions</u> Kristina Moffitt; Senior Emergency Services Coordinator, Cal EMA | 60 minutes |
| <u>Q&A and Closing</u> | 10 minutes |

Opening Remarks

- **Happy New Year!**
- **Status of AIO/AISO Meetings**
- **Security Program and Policy Improvement Sub-Committee**



Keith Tresh, Director and CISO

Organizational Update

- More organizational change on the horizon
- Governor's budget proposes to restructure Technology, General Services, and Human Resources into a new Government Operations Agency.
- Proposed changes are available at: <http://www.ebudget.ca.gov/>

Organizational Update (*Continued*)

■ Technology Agency supports the proposal.

“By placing the Technology Agency together with the Department of General Services and the Department of Human Resources, the opportunity to collaborate on issues such as IT procurement and maintaining a capable IT work force becomes easier.”

– Carlos Ramos, Secretary

Status on Required Security Reporting Activities

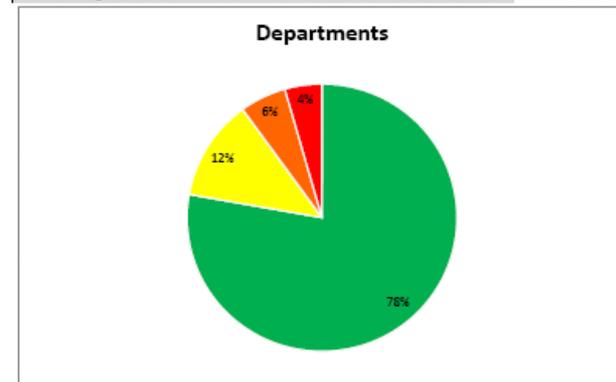
- Annual Filings Due January 31
- Next publication February 2012
- Use January 2012 form version accessible at http://www.cio.ca.gov/OIS/Government/activities_schedule.asp

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 Annual Security Activities Reporting (Continued)

| Annual Activity | Purpose | Value/Benefit to Agencies |
|--|--|---|
| Designation Letter | Ensure Agency has assigned personnel to fulfill key security and privacy roles and responsibilities. Also provides OIS ability to reach appropriate individuals for incident prevention, detection and response. | Receive notification of significant events affecting or potentially affecting them. |
| Risk Management and Privacy Program Compliance Certification | OIS mandate to track, monitor and report on state agency compliance with program requirements. | Statewide metrics and trends |
| Telework and Remote Access Security Compliance Certification | OIS mandate to track, monitor and report on state agency compliance with program requirements. | Statewide metrics and trends |
| Disaster Recovery Plan | Ensure Agency has a plan to recover critical/essential IT | Ability to minimize impact and recover within RTOs/MAOs |

Statewide Program Update

■ DR Management

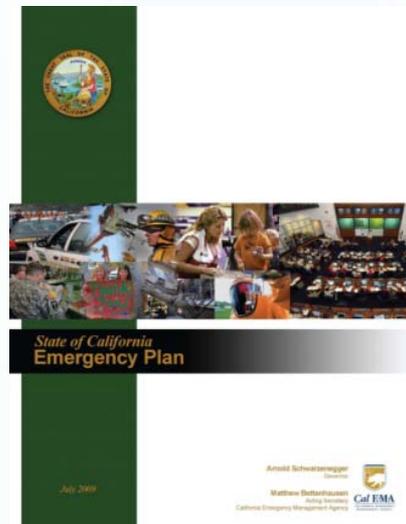
- DR Plan Reviews – Delays in review/feedback
- Process Overview

| All Submissions | Action Required Feedback on Last Full Submission | Feedback Pending on Last Full Submission |
|---|---|--|
| <p>Email acknowledges receipt of plan submission.</p> | <p>If agency has received OIS feedback on its last full plan submission, and feedback indicated ACTION REQUIRED, then the agency needs to either submit another full plan, and/or remediation plan, that addresses the deficiencies that were identified by its next submission due date. The submission must be signed by the Director or designee.</p> | <p>If agency has not yet received OIS feedback on its last full plan submission (<i>before the next plan submission due date</i>) and there have been no changes to the environment that would warrant updates to the plan, then the agency may submit a “No-change Certification”.</p> |

State Emergency Plan **California Emergency Functions**

Kristina Moffitt

Senior Emergency Services Coordinator, Cal EMA



Cyber Security Resources (1)

- **California Office of Information Security (OIS):**
 - An Office within the California Technology Agency.
 - The primary state government authority in ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information.
 - Represents the State to federal, state, and local government entities, higher education, private industry, and others on security-related matters.
 - Partners with people inside and outside of government to build a secure information security foundation.
 - <http://www.cio.ca.gov/OIS/>

Cyber Security Resources (2)

- **Department of Homeland Security's (DHS) National Cyber Security Division (NCSD):**
 - Established by DHS to serve as the federal government's cornerstone for cyber security coordination and preparedness, including implementation of the *National Strategy to Secure Cyberspace* .
 - Works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets.
 - Assists State and local governments in bolstering their cyber security capabilities.
 - Has identified two overarching strategic objectives:
 - Build and maintain an effective national cyberspace response system.
 - Implement a cyber-risk management program for protection of critical infrastructure.
 - www.dhs.gov/xabout/structure/editorial_0839.shtm

Cyber Security Resources (3)

- **U.S. Computer Emergency Readiness Team (US-CERT):**
 - Mission is to improve the nation's cyber security posture, coordinate cyber information sharing and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.
 - Partners with private sector cyber security vendors, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local governments, and domestic and international organizations.
 - Coordinates defense against and responses to cyber attacks across the Nation by collaborating with State and local Governments and sector information sharing and analysis centers (ISACs).
 - Serves as the operational arm of the NCSD analyzing cyber threats and vulnerabilities and disseminating cyber threat warning information.
- www.US-CERT.gov

Cyber Security Resources (4)

■ National Institute of Standards and Technology (NIST):

- Is a Federal agency within the U.S. Commerce Department's Technology Administration.
- Develops and promotes measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
- In order to build trust and confidence in information technology systems, the NIST Computer Security Division (CSD) provides standards and technology to protect information systems against threats to the:
 - Confidentiality of information,
 - Integrity of information and processes,
 - Availability of information and services.

Cyber Security Resources (4)

- **National Institute of Standards and Technology (NIST) Computer Security Division (CSD):**
 - Is one of six NIST divisions.
 - Responds to the Federal Information Security Management Act of 2002 (FISMA).
 - Provides assistance in using NIST guides to comply with FISMA.
 - Provides a specification for minimum security requirements for Federal Information and information systems using a standardized, risk-based approach.
 - Defines minimum information security requirements for information and information systems.
 - Federal Information Processing Standards (FIPS) publications are issued by NIST for use government-wide.
 - www.nist.gov

Cyber Security Resources (5)

■ **National Association of State Chief Information Officers (NASCIO):**

- Represents state chief information officers and information technology executives and managers from state governments across the United States.
- Mission is to foster government excellence through quality business practices, information management, and technology policy.
- Primary state members are senior officials from state government who have executive-level and statewide responsibility for information technology leadership.
- Provides state CIOs and state members with products and services designed to support the challenging role of the state CIO; stimulates the exchange of information; and promotes the adoption of IT best practices and innovations.
- www.nascio.org

Cyber Security Resources (6)

- **Multi-State Information Sharing and Analysis Center (MS-ISAC):**
 - The MS-ISAC is designated by the U.S. Department of Homeland Security (DHS) as the ISAC for state, local, territorial and tribal (SLTT) governments.
 - Its mission is to improve the overall cyber security posture of state, local, territorial and tribal governments.
 - Collaboration and information sharing among members, private sector partners and the DHS are the keys to success.
 - The OIS is California's state member representative.
 - <http://msisac.cisecurity.org/>

Training Resources

■ Free Online Training:

■ DHS/FEMA State Cyber Security Training

- Online, self-paced Cyber-Security training
- Available at no charge to US citizens
- <http://www.teexwmdcampus.com/index.k2>

IA General / Non-Technical:

- Information Security for Everyone
- Cyber Ethics
- Cyber Law and White Collar Crime

IA Technical / IT Professional:

- Information Security Basics
- Secure Software
- Network Assurance Digital Basics

IA for Business Professionals:

- **Business Information Continuity**
- Information Risk Management
- Cyber Incident Analysis and Response

Training Resources (*Continued*)

- **Government Mobility Forum:**
 - February 8, 2012
 - Sacramento Convention Center
 - Free to government employees
 - Register at: www.governmentmobility.net

Free Resources

■ Disaster Recovery Institute International

- www.drii.org/thrive/#/10/
- www.drii.org/docs/USBusinessContinuity.pdf

■ Disaster Recovery Journal

- <http://www.drj.com/>

■ Disaster Resource Guide

- <http://www.disaster-resource.com/>
- http://www.disaster-resource.com/index.php?option=com_user&view=register

Open Discussion

Friendly Reminders

FOUO Reminder:

- 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

Friendly Reminders (*Continued*)

DR Coordinator Meeting Changes Reminder:

- Registration is required so that we may:
 - More accurately account for the number of hand-outs / materials.
 - More easily track attendance/participation.
- A link is included in the meeting notice sent to DR Coordinators, back-ups, and interested parties on designee list.
- **DR Coordinators may forward to others**

Friendly Reminders (*Continued*)

Feedback Survey Reminder:

- **The meeting survey will be emailed to you.**
- **Please complete.**
- **Your feedback is important to us!**

Closing

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