

# **Disaster Recovery Coordinators' Meeting**

January 19, 2011

# Meeting Agenda

- ☑ Welcome
- ☑ Continued Impact of Hiring Freeze
- ☑ Policy Update –  
ITPL 10-02, ITPL10-03, ITPL 10-13, ITPL 10-14, ITPL 10-19  
([http://www.cio.ca.gov/Government/IT\\_Policy/ITPL.html](http://www.cio.ca.gov/Government/IT_Policy/ITPL.html))  
and SIMM 70B, 70D Form Updates, SIMM 65A Update In Progress  
(<http://www.cio.ca.gov/OIS/Government/policy.asp>)
- ☑ Legislative Update - AB 2091, AB 2408, SB 1055  
(<http://www.cio.ca.gov/About/legislation.html>)
- ☑ Security Compliance Reporting  
(<http://www.cio.ca.gov/OIS/Government/policy.asp>)
- ☑ Security Reporting Scorecard  
(<http://www.cio.ca.gov/OIS/Government/policy.asp>)
- ☑ Disaster Recovery Management – An Overview & What We Look For  
([http://www.cio.ca.gov/OIS/Government/disaster.asp#ORP\\_SAM](http://www.cio.ca.gov/OIS/Government/disaster.asp#ORP_SAM))

# Meeting Agenda - Continued



- ☑ Continuity Plans – Additional Criteria Related to the Emergency Management Accreditation Program (EMAP)  
(<http://www.emaponline.org/>)
- ☑ Cyber Exercises: Cabinet Level Tabletop Exercise and CyberStorm III
- ☑ California Cyber Incident Response Plan and New Cyber EF
- ☑ 2011 Federal Grants
  - ☑ Enterprise Business Impact Analysis (BIA):  
Critical Information Technology Infrastructure
- ☑ FEMA Challenge.gov ([www.challenge.gov/fema](http://www.challenge.gov/fema))
- ☑ DHS Public Service Announcement Challenge  
(<http://www.dhs.gov/files/events/stop-think-connect-psa-challenge.shtm>)
- ☑ Potential Agenda Items for Future Meetings (listed)

Q&A and Closing

# Continued Impact of Freeze

- Unable to fill behind positions vacated
- Will continue to wear multiple hats
- Impact to level of service and support
  - Response may be less timely
  - Will always have our great attitude
- Security scorecard color will not be affected when there has been a delay in OIS review and feedback

# Policy Update

([http://www.cio.ca.gov/Government/IT\\_Policy/ITPL.html](http://www.cio.ca.gov/Government/IT_Policy/ITPL.html))

- SAM/SIMM Updates You May Be Interested In:
  - Social Media (ITPL 10-02 Issued 2/26/10)
  - Telework and Remote Access (ITPL 10-03 Issued 3/2/10)
  - Security Reporting Scorecards (ITPL 10-13 Issued 10/4/10)
  - Data Center Consolidation (ITPL 10-14 Issued 10/29/10)
  - Smartphone (ITPL 10-19 Issued 12/30/10)
  - Required Security Reporting (SIMM Forms Updated)  
(<http://www.cio.ca.gov/OIS/Government/policy.asp>)
    - Forum held on 1/7/11
  - Disaster Recovery Plan Documentation for Agencies:  
Instructions - SIMM 65A (*update in development*)

# ITPL 10-14

## A Policy You Need to Know About!



### **DATA CENTER ASSIGNMENTS AND CONSOLIDATION**

**EMPHASIS:** Closure of Non-Tier III Data Centers and Server Rooms

([http://www.cio.ca.gov/Government/IT\\_Policy/ITPL.html](http://www.cio.ca.gov/Government/IT_Policy/ITPL.html))

Chapter 404, Statutes of 2010 ([AB 2408](#)) specifies that mission critical and public facing applications transition to Tier III data centers designated by the OCIO, and that all other existing server rooms are to be closed by June 2013.

AB 2408 defines targets and timelines for IT consolidation across the executive branch, **including email services**.

All Executive Branch state agencies are required to comply with AB 2408.

# ITPL 10-14 – CONTINUED



Executive branch agencies and departments must be in migration to the state shared email solution by June 2011:

- CA.Mail solution hosted at the Office of Technology Services
- California Email Services (CES) contract hosted by Microsoft

The following is the state's policy for determining an agency's Tier III-equivalent facility assignment:

The **Hawkins Data Center**:

- Department of Justice
- California Criminal Justice Information System's (CJIS)
- California Law Enforcement Telecommunications System (CLETS)

# ITPL 10-14 – CONTINUED



Department of Water Resources Data Center:  
Natural Resources Agency and its associated departments.

Franchise Tax Board (FTB) Data Center:  
FTB

Office of Technology Services (OTech) facilities:

Gold Camp Data Center:

- Executive Branch
- Managed Services
- Disaster Recovery Services

Federated Data Center (FDC):

- Shared by Agencies

Vacaville Data Center:

- Disaster Recovery
- Production Data Center

# ITPL 10-14 – CONTINUED



To facilitate timely completion of consolidation activities:

- OTech Customer Owned Equipment Managed Services (COEMS) discontinued
- Departmental server rooms will be closed by June 30, 2013.
- New applications, server refreshes, storage replacements, and new virtualization clusters shall be located at a state Tier III facility.
- Agencies shall review all IT projects in progress in order to plan transition of servers and storage to a state Tier III facility.
- The Computer Room Construction policy and requirements established in ITPL 09-04 remain in effect.
- Facility upgrades for server rooms designated for shutdown are limited to emergencies.
- Agencies shall utilize the approval procedures described in [ITPL 09-04](#) (Data Center Construction).

# Legislative Update



<http://www.cio.ca.gov/About/legislation.html>

AB 2091

[http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab\\_2051-2100/ab\\_2091\\_bill\\_20100827\\_chaptered.html](http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_2051-2100/ab_2091_bill_20100827_chaptered.html)

PRA Exemption

Approved by the Governor & Chaptered 8/27/2010

AB 2408

[http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab\\_2401-2450/ab\\_2408\\_bill\\_20100928\\_chaptered.html](http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_2401-2450/ab_2408_bill_20100928_chaptered.html)

OCIO - California Technology Agency

Approved by the Governor & Chaptered 9/28/2010

SB 1055

[http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb\\_1051-1100/sb\\_1055\\_bill\\_20100924\\_chaptered.html](http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1051-1100/sb_1055_bill_20100924_chaptered.html)

California Technology Agency Fingerprint

Approved by the Governor & Chaptered 9/24/2010

# Legislative Update

## AB 2091



- Public Records Act (PRA) exemption
- Information Security records that would reveal vulnerabilities or would increase the potential for an attack on an information system
- Although AB 2091 does limit the public's right of access, it is a very limited and targeted exemption

# Legislative Update

## AB 2408



- Governor's Reorganization Plan clean-up bill
- Codifies Executive Order S-10-03
- Name change – OCIO to California Technology Agency
- Extends California Technology Agency's sunset set date from 2013 to 2015
- Imposes additional duties on the Secretary of the California Technology Agency.
- Strengthens the OIS's oversight and enforcement authority.

# Legislative Update

## SB 1055



- California Technology Agency - fingerprints and criminal history checks.
- California Technology Agency employees and contractors that have access to sensitive or confidential information.
- Conviction of crimes related to dishonesty, fraud, or deceit and is substantially related to the duties of the person.
- There is an appeals process.

# Security Compliance Reporting 2011

1/31/2011 SIMM Forms Due



All SIMM forms except the Agency Information Security Incident Report have been updated.

**Agencies are to use the updated versions for Jan 2011! Outdated forms will be rejected.**

Report/Activity	Policy Section	Instructions and Forms	Due Date
Agency Designation Letter	5360.1	<a href="#">SIMM 70A</a>	Annually by January 31 <u>and</u> within ten (10) business days of any change in designee
Agency Risk Management and Privacy Program Compliance Certification	5360.1	<a href="#">SIMM 70C</a>	Annually by January 31
Disaster Recovery Plan (Complete)	5360.1	<a href="#">SIMM 65A</a> <a href="#">SIMM 70D</a>	Annually pursuant to the <a href="#">DRP Submission Schedule</a>
Disaster Recovery Plan Certification (No-Change)	5360.1	<a href="#">SIMM 70B</a>	Every-other year pursuant to the <a href="#">DRP Submission Schedule</a> in lieu of a complete plan when no changes have occurred since last submission.
<hr/>		<a href="#">SIMM 65B</a>	
Agency Information Security Incident Report	5360.1	<a href="#">SIMM 65C</a> <a href="#">SIMM 65D</a>	Within ten (10) business days from the date of notification to CHP's Emergency Notification and Tactical Alert Center (ENTAC)
Agency Telework and Remote Access Security Compliance Certification	5340	<a href="#">SIMM 70E</a>	Initial by July 1, 2010. Annually by January 31 thereafter, commencing January 31, 2011.

# Security Compliance Reporting 2011 Continued



**Purpose** of reporting is to ensure agency

- Understands its responsibility for security
- Is aware of and is appropriately managing risk
- Is implementing timely and appropriate corrective actions
- Is achieving regulatory and policy compliance
- Is ensuring the trust of Californians by protecting the State's information assets

It's NOT just about filling in or checking the boxes!

## **Expectations**

- All agencies subject to compliance with state policy and standards, and Government Code Sections 11546.1 and 11549 et.seq. will participate
- Others are strongly encouraged to voluntarily participate

# Security Compliance Reporting 2011 Continued



## **Benefits** of participation

- Promotes the entity's recognition and support for the state's need to understand its security posture across all state entities.
- Entity will receive credit for participation through scorecard.
- Entity receives other benefits. For example, Designation Letter provisions for critical alert and emergency notifications.

# Security Compliance Reporting 2011 Continued



## Where to Access Current Forms ?

A screenshot of a web browser displaying the "Policy" page of the California Office of Information Security. The browser's address bar shows the URL "http://www.cio.ca.gov/OIS/Government/policy.asp". The page header includes the "CA.GOV" logo and "Office of Information Security". A navigation menu contains "Home", "Government", "About Us", and "Contact Us". Below this is a secondary menu with "Mission", "Governance", "Policy", "Disaster Mgmt", "Incident Mgmt", "Risk Mgmt", "Privacy", "Go RIM", "Events", and "Library". The main content area is titled "Policy" and includes an "Overview" section. This section contains a paragraph of text and a list of links: "State Administrative Manual (SAM)", "Statewide Information Management Manual (SIMM)", "Management Memos", "Budget Letters", "Go RIM", "Now Vetting", "Definitions", and "Compliance". The "Compliance" link is circled in red. Under "Compliance", there are three sub-links: "Schedule of Required Reporting Activities", "Schedule for Submission of Disaster Recovery Plans", and "Security Reporting Scorecards". On the left side of the page, there are sections for "ACTING STATE CIO CHRISTY QUINLAN", "ACTING CHIEF INFORMATION SECURITY OFFICER KEITH PARKER", and a "CYBER THREAT LEVEL" section with a "LAUNCH NOW!" button and a "GUARDED" status. A "Text version" link and a list of RSS feeds and videos are also visible.

<http://www.cio.ca.gov/OIS/Government/policy.asp>

# Security Reporting Scorecard



## Initial Scorecards Based On:

- Four required submissions
  - Designation Letter (SIMM 70A)
  - Risk Management and Privacy Program Compliance Certification (SIMM 70C)
  - Disaster Recovery Plan **and** Transmittal Letter (SIMM 70D) **or** Disaster Recovery Plan Certification (SIMM 70B)
  - Telework and Remote Access Security Compliance Certification (SIMM 70E)
- Receipt only

## Later Scorecards *Will* Include:

- Voluntary participation

## Later Scorecards *May* Include:

- Completeness of submissions
- Timeliness of submissions

# Security Reporting Scorecard Continued

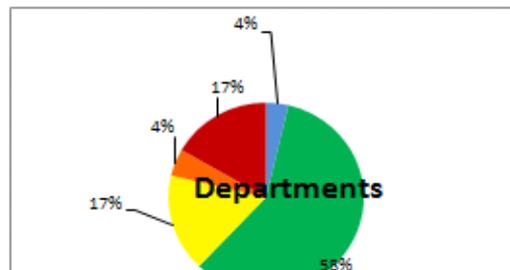
## Agency Security Filing Compliance - November 2010

Agency	Compliant	In Progress	No Progress	Filing Progress
<u>BTH</u>	11	2	1	86%
<u>CDCR</u>	1	1	1	50%
<u>EPA</u>	5	1	0	92%
<u>HHS</u>	14	1	0	97%
<u>LWDA</u>	5	1	1	79%
<u>Resources</u>	7	11	8	48%
<u>SCSA</u>	8	4	0	83%
<u>Other</u>	16	2	7	68%
<b>State Total</b>	<b>67</b>	<b>23</b>	<b>18</b>	<b>73%</b>

Scorecard	Departments
Blue	4
Green	63
Yellow	18
Orange	5
Red	18

### Scorecard Status Key

- BLUE** - Compliant - All filings received and fully accepted.
- GREEN** - Compliant - All filings received and are pending OIS review.
- YELLOW** - At Risk - One filing not received.
- ORANGE** - At Risk - Two or three filings not received.
- RED** - No filings received.



Sample

# Security Reporting Scorecard

## Continued



### Legend

<b>Red</b>	No Progress
<b>Orange</b>	At risk - two or three items missing.
<b>Yellow</b>	At risk - one item missing.
<b>Green</b>	Compliant - All filings received and are pending OIS review.
<b>Blue</b>	Compliant - All filings received and fully accepted.

# SAM 5355

## Disaster Recovery Management

[http://www.cio.ca.gov/OIS/Government/disaster.asp#ORP\\_SAM](http://www.cio.ca.gov/OIS/Government/disaster.asp#ORP_SAM)

### SAM 5355 does what?

These policies are designed to ensure processes and procedures are in place to ensure an agency's ability to continue its essential functions during a business disruption or major catastrophic event.

Disaster Recovery (DR) Planning provides for continuity of computing operations in support of critical business functions following a business disruption.

# SAM 5355.1

## Disaster Recovery Planning

- It is essential that critical IT services and applications be restored ASAP.
- DR planning is based upon available knowledge and assumptions, and must be adapted to changing circumstances and business needs and updated routinely to anticipate risks and threats.
- The DR planning process should include the results of Risk Analysis (RA) and Business Impact Analysis (BIA) when developing Disaster Recovery Plans (DRP).
- To provide for recoverability of new systems, all agencies must include disaster recovery considerations and costs in project authority documents and budget proposals.

# SAM 5355.2

## The Disaster Recovery Plan



- Each state agency must maintain a DRP identifying the computer applications that are critical to agency operations, the information assets that are necessary for those applications, and the agency's plans for resuming operations following an unplanned disruption of those applications.
- Each agency that employs the services of a state data center must develop an understanding of the existing service level agreement for recovery services and its recovery plan must document the data center services that will be required during recovery.
  - DRPs must include recovery agreements and coordinating procedures with the data center.

## SAM 5355.2 - Continued



- Each agency must file a copy of its DRP and the signed Agency DRP Transmittal Letter (SIMM 70D) with the Office of Information Security in accordance with the DRP submission schedule.
- If the agency employs the services of a state data center, it must also provide the data center with either a full copy or a subset of its plan, containing enough information for the data center to recover the agency's systems and/or data.
  - For example, OTech is responsible for OTech's equipment, but agencies are responsible for their own applications and data that resides at OTech.
  - An agency is either subscribed to OTech's DR Service or it isn't.
    - *If subscribed*, recovery of pre-identified applications and data will occur within 72 hours at an IBM recovery center, or up to 8 hours in the Vacaville Data Center.
    - *If not subscribed*, Otech will need additional information about applications and data in order to recover 3-6 months later at IBM, or a month or more at the Vacaville Data Center.

# SAM 5355.2 - Continued



- A signed Agency DRP Certification (SIMM 70B) may be filed in place of a full DRP if both of the following conditions exist:
  - A full plan was submitted the previous year and is on file with the Office (the OIS will keep the latest copy on file due to recent PRA legislation that protects DRP's).
  - AND no changes are needed to the current plan.

# SAM 5355.2 - Continued

## SIMM 65A



- Each agency DRP must cover, at a minimum, ten topic areas listed and described in the Disaster Recovery Plan Preparation Instructions (SIMM 65A).
- If the agency has not developed a full Continuity Plan (required by CalEMA), or if the following items have not been captured in the Continuity Plan, three supplemental DRP requirements must be met.
  - Damage recognition and assessment.
  - Mobilization of personnel.
  - Primary site restoration and relocation.
- If the DRP does not follow the format outlined in SIMM 65A, a cross-reference sheet (attached to SIMM 70D previously discussed) must be included with the update to indicate where information on each topic area can be found in the DRP.

# SAM 5355

## Disaster Recovery Management



- Each department is responsible for ensuring a DRP or DRP Certification is filed in accordance with the DRP submission schedule.
- If a DRP or DRP Certification is not filed by the DRP submission schedule date, that deficiency will be noted on the agency reportcard that has been posted to our website beginning November 2010.
- If a DRP does not meet the minimum requirements, the agency will be notified and recommendations will be supplied. Deficiencies will not be reflected on report card status until February 2012.
- The OIS will provide assistance in a limited consulting capacity to ensure understanding of requirements and content, and to answer questions about whether the agency's approach meets requirements.
- The OIS is considering aligning all department submittal dates with their associated Agency submittal date. Any objections?

# SAM 5355.2

## DRP – What we Look For



- *Either* an Agency DRP Transmittal Letter (SIMM 70D) or DRP Certification (SIMM 70B) form **either one signed by the agency secretary/director, or by a SIMM 70A pre-identified designee,** delivered in accordance with the DRP submission schedule.
- Compliance with SAM requirements and SIMM 65A format (refer to cross-reference sheet/checklist to be sure).
- Exercise schedule, description, results, remediation plans. Must perform alternate exercise every other year.

# SAM 5355.2 - Continued



- Critical inter and intra departmental dependencies such as those with a state data center, SCO, SPB, DOF, etc. and coordinating recovery procedures.
- Critical data/applications housed at a state data center and recovery plans and procedures for those, and inter-relationships between the data center plan and your agency plan with coordinating recovery procedures.
- Specific recovery procedures for essential/critical data/ applications for your employees to follow – remember, your primary SME may not be available! This is your agency’s plan for recovery, and procedures must be clear enough for anyone technically savvy enough to follow and recover your IT systems!

# Continuity Plans

## Additional Criteria Related to the Emergency Management Accreditation Program (EMAP)



According to Executive Order S-04-06, state executive branch agencies must submit a Continuity Plan based on guidelines issued by CalEMA. The guidance Cal EMA published was based on the federal continuity model (guidance), which lists and describes the following ten essential elements of Continuity Plans:

- Identification and Prioritization of Essential Functions
- Lines of Succession
- Delegation of Authority
- Alternate Facilities
- Communications
- Vital Records and Databases
- Human Capital
- Tests, Training and Exercises
- Devolution
- Reconstitution

# Continuity Plans - Continued



During recent discussions with CalEMA, we've come to believe that they are aiming for the Emergency Management Accreditation Program (EMAP) certification, a standard-based assessment and peer review accreditation process for government. (<http://www.emaponline.org/>) This program adds seven additional criteria for comprehensive Continuity Plans:

- Purpose, Scope and Goals
- Authority
- Situation and Assumptions
- Functional Roles and Responsibilities
- Logistics Support
- Concept of Operations
- Plan Maintenance

We have heard no formal request from CalEMA for all agencies to participate, but thought you should be aware this may be their future direction. Check with your CalEMA representative to confirm.

# Cyber Exercises

## Cabinet Level Cyber Tabletop Exercise



Three hour cyber emergency management tabletop exercise October 26, 2010

Led by Good Harbor Consulting and Co-Sponsored by:

- CalEMA
- Office of Information Security

20+ California state agencies participated including:

- Emergency Management, Finance, IT, Public Health and Natural Resources

Lessons Learned included:

- Identifying mission-critical data and prioritizing recovery across all agencies
- Guaranteeing the availability and delivery of mission-critical functions
- Improving incident detection and reporting at the state level

# Cyber Exercises - CyberStorm III



California participated as a “full player” in Cyber Storm III

- California Technology Agency’s Office of Information Security (OIS)
- California Emergency Management Agency (CalEMA)
- Five State agencies
- Sacramento local government
- Palo Alto local government
- Infragard

Goals:

- Identify DHS’s role in its National Cyber Incident Response Plan (NCIRP)
- How to link state plans to the National plan
- Test the effectiveness of California State Cyber Incident Response plans and procedures
- Determine how to better coordinate with the Federal and local governments, other States, communities, and private partners.

# Cyber Exercises - CyberStorm III Continued



Injects included:

- multiple infected hosts
- phishing
- website defacements
- extortion
- compromised DNS records
- redirections to hacker sites
- botnets
- all ca.gov websites down
- OTech hosted email inoperable

# Cyber Exercises - CyberStorm III Continued - Findings



After Action meetings at the State and National levels revealed:

The need to improve methods for information sharing.

The need for establishing more formal relationships with:

- CalEMA
- State Fusion Center
- DHS National Cyber Security Division (NCSD)
- DHS National Cybersecurity and Communications Integration Center (NCCIC)

The need to develop a California cyber incident response plan:

- A draft California Cyber Incident Response Plan (CCIRP) tied to the State Emergency Plan (SEP) is in the early stages of development.
- The draft CCIRP has been delivered to CalEMA and to the OIS
- Key cabinet and executive level decision makers as well as public and private sector partners will need to be involved.
- Establishment of a workgroup will be required in further development of this plan.

# Cyber Exercises - CyberStorm III

## Continued - Findings



The need for a California Cyber Emergency Function (EF) within the SEP

- If a new Cyber EF is formally adopted, the CCIRP will reside within this EF

The need for an Information Sharing and Analysis Center (ISAC) web portal

- This would need Federal funds to establish and maintain

The need for a California Information Security Operations Center (CA-ISOC)

- This would need Federal funds to establish and maintain

# California Cyber Incident Response Plan (CCIRP)



The purpose of this plan is to support the State of California's public policy of:

- Preparing for, and responding to, all Incidents of Statewide Significance that threaten the safety of its citizens.
- Addressing the management of cyber incidents of statewide significance that are declared a disaster or an emergency for the State of California.
- Augmenting California's State Emergency Plan (SEP) that guides California's overall response to emergencies and disasters.
- State agencies will use this document to assist them in their planning activities for responding to all cyber emergencies including:
  - cyber incidents with a physical impact
  - physical incidents with a cyber impact

# CCIRP - Continued



## ***Scope***

- Provides direction to all state agencies within California
- Intended as guidance for local agencies
- Intended to clarify the roles and relationships of agencies at the state and federal levels of government in managing cyber incidents.

## ***Objectives***

- Outline the roles, responsibilities and capabilities of local, state and federal agencies in preparing for and responding to cyber incidents
- Provide planning, response, and recovery guidance that is consistent with the State Emergency Plan (SEP) and federal guidance
- Provide a basis for identifying required training of personnel and exercising of the State's capabilities for responding to cyber incidents

# 2011 OIS Federal Grant Requests



- 9 Security-related grant projects included in application
- Just over \$7.5 million
- Applications under review by CalEMA award committee
- Awaiting award announcement
- **Potential** grant request for 2012: assistance with DRP development for agencies, and a DR Coordinator training program.
- Meanwhile, a separate training session will be held for new DR Coordinators.
- Until then, we suggest use of SIMM 65A guidance and collaboration with/borrowing from your partner/Agency departments.

# 2011 OIS Federal Grant Request

## Enterprise Business Impact Analysis (BIA): Critical Information Technology Infrastructure



By implementing an enterprise-wide BIA and gap analysis focused on California State Government's enterprise mission-critical information technology infrastructure across all state agencies, California can achieve the following objectives:

- Identification of known threats, vulnerabilities and potential consequences of disasters and attacks against the State's critical information technology assets and infrastructure and to the enterprise
- Measurement of the effectiveness of current controls to mitigate known threats, and the effects of risk-mitigation actions on not only the threat, but also on state government business operations
- Help consolidate the disparate, redundant, siloed and costly threat and IT disaster management operations across the state that do not adequately address threats. Yielding improvements over California's current siloed information technology disaster recovery/information systems contingency planning practices and yield better, more actionable information to the state.

# 2011 OIS Federal Grant Request Continued



- Provide increased transparency and accountability into how government is protecting critical information technology infrastructure
- Identify additional technology-based options and networks to provide further communications interoperability, and ensuring redundancy of existing technology-based critical state emergency communications systems for use by emergency responders
- Improve the state's continuity planning and IT disaster recovery/information systems contingency planning, response and recovery capabilities based on concrete knowledge of key threats – recommend better coordinating the state's Continuity Planning and Disaster Recovery programs.

# 2011 OIS Federal Grant Request Continued



- Create a repeatable process that will become the foundation for all Business Impact Analyses for the state, which will provide standard, common set of skills for threat and IT disaster management within state agencies
- Recommend better coordinating the State's Continuity Planning and Disaster Recovery programs
- Prioritization of remediation and recovery activities required to mitigate known vulnerabilities/threats to acceptable levels. Prioritize and direct funding, technology and specialized resources towards high-threat IT areas to the enterprise as a whole. Recommendations for recovery priorities based on criticality of networks/systems/data

# 2011 OIS Federal Grant Request Continued



- Identification of, and mitigation strategies for, critical interdependencies between and among agencies.
- Present executive leadership and legislators an enterprise-level view into the resiliency of the State of California's critical IT infrastructure and the IT health of the state based on objective, standardized cross-agency data gathered in the BIA/gap analysis
- Enable leadership to answer the question:
  - "Are currently deployed information-protection controls reasonably adequate to mitigate risks to critical infrastructure and if not, what control enhancements are justified?"



**Challenge.gov** beta  
Government Challenges, Your Solutions



Federal Emergency Management Agency (FEMA) announced a new public challenge to come up with creative ideas on how we can prepare communities before disaster strikes. FEMA discussed how responding to disasters takes an entire team, not just the U.S. government, and how we must plan for the entire community before disaster strikes.

FEMA is encouraging all members of the public to participate and submit their ideas by visiting [www.challenge.gov/fema](http://www.challenge.gov/fema).

The sky is the limit. This could be a new project or means of engaging the public to prepare for disasters on the individual or family level; **a public service announcement about business preparedness to play on local radio or TV stations; or a new device, technology, application or piece of equipment to mitigate the effects of disaster**. Submissions will be judged based on originality, level of community engagement and ease of implementation.



**Challenge.gov** beta  
Government Challenges, Your Solutions



Submission Period: **Start:** Oct 28, 2010 12:00 AM EDT **End:** Jan 29, 2011 11:59 PM EST Judging Period: **Start:** Jan 31, 2011 12:00 AM EST **End:** Feb 18, 2011 11:59 PM EST Winners announced: Feb 22, 2011 12:00 AM EST. The Winner The best, most unique idea will be selected as the winner and will be highlighted on FEMA's website.

Earlier this year, FEMA put together the first ever Technology Sector Day, as a forum to bring government and key technology innovators together to discuss how to work better together and how to leverage technology to improve the way FEMA does business. Participants included tech giants such as Google, Microsoft, Facebook, Verizon and others.

# Department of Homeland Security Public Service Announcement Challenge



## **Stop. Think. Connect.** PSA Challenge:

- DHS challenge kicked-off November 8, 2010
- Looking for videos that:
  - will educate Americans about Internet safety.
  - inspire Americans to **Stop. Think. Connect.**

## **Challenge Deadline:**

Monday, February 14, 2011, at 11:59 p.m. ET.

## **Categories:**

PSAs directed towards any of the following audiences:

- Teenagers (13-17)
- Young Adults (18-24)
- Parents of Teenagers
- Older Americans

## **More information about how to participate:**

<http://www.dhs.gov/files/events/stop-think-connect-psa-challenge.shtm>

# Requested Topics for future DR Coordinator Meetings:



- Potential 2012 grant request for DRP assistance and DR training
  - Disaster Declaration Procedures
  - Two-factor authentication and twitter in DR situations
  - Exercise Planning
  - Business Impact Analysis/Business Impact Studies/Risk Assessment
  - DRP Examples (will anyone offer to share?)
  - DRP Challenges
  - Continuity Planning (CaEMA) vs DR Planning (OIS)
  - SEMS/NIMS
  - LDRPS/eBRP/Emergency Notification Systems Presentations
  - Future Requirements
  - DRP Workshops, Section-by-Section
  - How do you coordinate between departmental DR and BC Plans?
  - OTech Training Offerings (HALO, GoOnline, Classes)
  - DR Training Resources and Opportunities
    - [mile2.com/Disaster\\_Recovery\\_Planning\\_and\\_Business\\_Continuity\\_Planning\\_Training.html](http://mile2.com/Disaster_Recovery_Planning_and_Business_Continuity_Planning_Training.html)
    - <https://www.drii.org/>
    - [www.sentryx.com](http://www.sentryx.com)
    - [www.onlinecontinuity.com](http://www.onlinecontinuity.com)
    - [www.disasterrecoveryworld.com](http://www.disasterrecoveryworld.com)
    - Association of Sacramento Area Planners <http://www.asapsite.org/>
    - Statewide Emergency Planning Committee [http://cms.calema.ca.gov/prep\\_swepc.aspx](http://cms.calema.ca.gov/prep_swepc.aspx)
- Next Mtg January 26, 2011; (916) 845-8781 - [diane.kuncz@calema.ca.gov](mailto:diane.kuncz@calema.ca.gov)

# Questions



# Closing



- Feedback
  - New method for meeting evaluations.
  - You will receive an email with a link to a Zoomerang survey.
  - We appreciate your feedback.
- Next Meeting
  - April 20, 2011
  - Tentative Special Guest: OTech: New DR Service Offering