

# Bits and Bytes

Tidbits of information for  
Information Security Officers  
January 2009



## WHAT'S NEW FROM OUR OFFICE!

- **Compliance Requirements** - Agency Designation Letter (SIMM 70A) and Agency Risk Management and

Privacy Program Compliance Certification (SIMM 70C) are **due to OISPP by February 2, 2009**. The newly revised forms must be used. Older versions will be returned to the agency.

- **Information Sheets**

Telework Security Considerations - which will help your agency consider security risks associated with telework. Also check out the related DGS resources on their website at

<http://www.dgs.ca.gov/Telework/Resources.htm>

Does Your Agency Implement Forced Password Changes? - which explains the importance of adopting a policy of a 30 to 90 day password expiration to meet the current standards, policies, and practices adopted by the state.

All the Information Sheets OISPP releases can be found on our web site at <http://www.oispp.ca.gov/government/library/awareness.asp#info-sheets>

- **Videos Web Page** on our web site at <http://www.oispp.ca.gov/government/video/default.asp> has lots of good video clips on disaster recovery, security awareness, and risk management.
- **Alerts Feed** on our web site at <http://www.oispp.ca.gov/government/default.asp> which provides immediate access to US-CERT, MS-ISAC and U.S. Department of Homeland Security vulnerability alerts and other pertinent information.

## UPCOMING EVENTS/TRAINING OPS

Watch for more information on these training opportunities.

- January 21, 2009 - DTS Quarterly Security Forum
- February 5, 2009 - 9:30-11am - Ethical Hacking Presentation by SANS, at the EDD Auditorium
- March 16<sup>th</sup> - 20<sup>th</sup>, 2009 - Free CISSP CBK Review Course - See OISPP for details

- OISPP is in the process of scheduling free federal training for:
  - Incident Response
  - Incident Detection and Deterrence
- Information Security Leader Academy (ISLA) kicks off in May 2009
- Join OISPP's Disaster Recovery quarterly meetings
  - Contact OISPP for details



## OISPP'S EMAIL DISTRIBUTION LIST - SUBJECT LINE STRUCTURE

OISPP has developed an internal subject line structure that will hopefully help people on our distribution lists

better manage email they receive from us (at least be able to better distinguish between something that needs to be acted upon right away versus something that can wait) since some information OISPP sends is just an FYI, while others require action. The following are the subject line introductions OISPP is using, along with examples for their use:

- FYI - *Announcements about forms updates, guidance documents, newsletters*
- SITUATIONAL AWARENESS - *Early warning about actual or potential threats*
- ACTION REQUIRED - *SIMM follow-up/due, remediation supplemental/status required, and vulnerability alerts and advisories with a Low or Medium risk rating*
- IMMEDIATE ACTION REQUIRED - *Critical and out of Band updates, patches, vulnerability alerts and advisories with a High risk rating*
- NO ACTION REQUIRED - *Acknowledgements for receipt of submitted documents, such as Disaster Recovery Plan submissions which meets requirement*
- POLICY ANNOUNCEMENT - *New or revised policy releases*
- TRAINING ANNOUNCEMENT - *Training opportunities*
- IMPORTANT REMINDER - *Annual filings*



## TO SKYPE OR NOT TO SKYPE!

Skype is typically used for telephone calls over the Internet, videoconferencing, and podcasts.

Agencies considering use of any technology must carefully consider and document the risks associated with the use of technology and their approach to the treatment of those risks (e.g., avoidance, mitigation strategies, acceptance, etc.). See State Administrative Manual (SAM) Section 5305, Risk Management at <http://sam.dgs.ca.gov/toc/5300/5305.htm>.

Although, our Office does not have an official stand on the use of Skype or any other particular technology considered for use in state government, OISPP offers the following recommendations and security concerns regarding the use of this particular technology:

- 1) Skype is a form of peer-to-peer (P2P) software. Per SAM Section 5310 - "Ensure that the use of peer-to-peer (P2P) technology for any non-business purpose is prohibited. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property. Business use of peer-to-peer technologies must be approved by the CIO and ISO."

Based on this policy, the use of P2P must be limited to legitimate business necessary application and properly managed to prevent copyright and intellectual property right infringement. The penalties in this area can be quite costly.

- 2) Although growing in popularity, Skype is well known for its security issues, including the ability for hackers to download Trojans to it for wiretapping and illegal monitoring purposes, allowing the potential for confidential/sensitive information to be improperly disclosed and the disruption or denial of essential business services.
- 3) In reviewing Skype's Privacy Statement on their web site at <http://www.skype.com/legal/privacy/general/>, there may be some concerns regarding how the individual's data is collected, used and shared with others. Review this Statement with your agency legal office to ensure it will not violate state or departmental policies.
- 4) OISPP recommends review of two information sheets it has recently released:
  - Use of Web Services Offerings ([http://www.oispp.ca.gov/government/document/s/pdf/Information\\_Sheet\\_4\\_Web\\_Service\\_Offerings.pdf](http://www.oispp.ca.gov/government/document/s/pdf/Information_Sheet_4_Web_Service_Offerings.pdf)) - which will help your agency weigh the benefits and risks of using a service such as Skype.
  - Telework Security Considerations ([http://www.oispp.ca.gov/government/document/s/pdf/Information%20Sheet\\_6\\_TeleWork\\_Security\\_Considerations\\_Nov\\_2008.pdf](http://www.oispp.ca.gov/government/document/s/pdf/Information%20Sheet_6_TeleWork_Security_Considerations_Nov_2008.pdf)) - which will help your agency consider some of the security risks associated with telework.



## USING THE LAST FOUR DIGITS OF AN SSN

With respect to printing the last four digits of a Social Security Number (SSN) instead of the entire SSN on mailed correspondence, consider Civil Code section 1798.85 in addition to the breach

notification requirements found in Civil Code section 1798.29. This section specifically prohibits the printing of a SSN, in whole or in part, on any materials mailed to the individual unless a state or federal law specifically requires the SSN be printed on the document to be mailed. There was a recent Presidential Executive Order (E.O.) that modified a longstanding order that required federal agencies to use the SSN. The new order now makes it permissive versus mandatory.

OISPP had sent an announcement about the new E.O. that was issued in November 2008 because it not only replaces the language which mandated the use of the unique identifier with more permissive language, it also establishes as Federal policy the requirement that agencies "should conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use." (73 Fed. Reg. 70,239, 11/20/08).

The breach notification section (1798.29) does not make a distinction between the entire SSN and partial SSN. Thus, it would be subject to legal challenge. However, in the context of today's other existing privacy laws and the risk it potentially presents to individuals, (having the name, address and last four digits of the SSN can provide access to financial, credit, or public utility accounts such as telephones, electricity, etc. as many creditors still use the last four-digits as a verification key for gaining access) OISPP believes it to be a bad practice. Further, absent any specific legal requirements for doing so, it appears to be a violation of Civil Code section 1798.85.

Due to the increased concerns by individuals about the use of their SSN, in whole or in part, and the increased level of scrutiny that breaches of personal information produce OISPP recommends that all state agencies eliminate the use of SSN altogether, unless specifically required by law.

## CONTACT US

Office of Information Security & Privacy Protection  
Attention: Office of Information Security  
1325 J Street, Suite 1650  
Sacramento, CA 95814  
(916) 445-5239  
[security@oispp.ca.gov](mailto:security@oispp.ca.gov)  
[www.infosecurity.ca.gov](http://www.infosecurity.ca.gov)

