

# Privacy/Security

# UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 16

SEPT. 2006

## Resources

### Privacy Program

(503) 945-5780

### Information Security

(503) 945-6812

### Information Security/ Privacy Web site

[www.oregon.gov/DHS/  
admin/infosec/](http://www.oregon.gov/DHS/admin/infosec/)

### Privacy Help Email

PrivacyHelp, DHS

### Information Security Email SECURITY, DHSINFO

### Privacy Policies

[www.dhs.state.or.us/policy/  
admin/privacypolicy.htm](http://www.dhs.state.or.us/policy/admin/privacypolicy.htm)

### Information Security Policies

[www.dhs.state.or.us/policy/  
admin/infosecuritylist.htm](http://www.dhs.state.or.us/policy/admin/infosecuritylist.htm)

*Send requests for  
future Privacy/Security  
Update topics to:*

*[dhs.privacyhelp@state.or.us](mailto:dhs.privacyhelp@state.or.us)*



## ISO or OIS? — That is the question (and here is the answer)

Acronyms are a way of life in state government. They help make our sentences shorter, but they can also create confusion. There appears to be some confusion between the acronyms used for the *Information Security Office (ISO)* and the *Office of Information Systems (OIS)*.

ISO and OIS — both housed on the fifth floor of the Human Services Building in Salem, and both having something to do with computer systems. Is it any wonder that there's confusion? Let's try to clarify.

### **Information Security Office Mission Statement:**

*“The ISO supports the department’s mission of assisting people to become independent, healthy and safe by providing leadership and services that assist DHS in securing the confidentiality, integrity, and availability of its information assets.”*

In other words, the ISO is focused on protecting confidential and other sensitive information from inappropriate access or disclosure, and ensuring that all DHS information assets are available to those who have the right and the need to access them. ISO assesses information security risks and works with OIS and business units to reduce or eliminate these risks. These risks may pertain to building security, business continuity, access control, information storage, awareness and education.

### **Office of Information Systems Mission Statement:**

*“Providing exceptional information services committed to fulfilling the DHS mission.”*

OIS technology services involve software and hardware, ensuring that DHS staff has the tools available to do their jobs. OIS focuses on improving the delivery and protection of electronic information.

**Take a related QUIZ on page 2...**

**Take the following quiz to learn more about the differences between ISO and OIS.** (Check your answers on page 4.)

1. *The Privacy Program is part of the:*
  - a. Information Security Office
  - b. Office of Information Systems
2. *You have a new staff person starting in your office. To request the AMD (Add, Modify, Delete) process you notify the:*
  - a. Information Security Office
  - b. Office of Information Systems
3. *You get to work and can't log on to your computer. It won't take your password, so you call the Service Desk, which is part of the:*
  - a. Information Security Office
  - b. Office of Information Systems
4. *There is some confusion and even a little conflict in your office about disclosing alcohol and drug treatment records without a client-signed authorization. For guidance you would call the:*
  - a. Information Security Office
  - b. Office of Information Systems
5. *The office you work in uses one generic password for the four support staff, which is kept on a "sticky" on the front of the reception desk computer. You remember a policy and something about not sharing passwords. For clarification and guidance on the policy you call the:*
  - a. Information Security Office
  - b. Office of Information Systems
6. *The email message you just received includes highly confidential information; client name, address, date of birth, Social Security number. You have no relationship to the client and none to the branch office that sent the message. It dawns on you that you should not have received that sensitive information, and you wonder if others also received it in error. The office which handles misdirected email is the:*
  - a. Information Security Office
  - b. Office of Information Systems
7. *You've been entering case notes into the TRACS system for three years. Nothing about your job description or duties has changed. The message that just popped up is that you are being denied access. To remedy this situation you call the:*
  - a. Information Security Office
  - b. Office of Information Systems
8. *You inadvertently access an illicit Web site from your computer at work. In order to diminish the risk of "infecting" both your computer and the DHS IT system, you should immediately call the:*
  - a. Information Security Office
  - b. Office of Information Systems
9. *You receive a phone call from someone identifying himself as being from the DHS-Info Technology Systems Team. They ask you for your RACF ID. The office that will handle this incident is the:*
  - a. Information Security Office
  - b. Office of Information Systems

## Privacy Contacts

### Privacy Officer

Jane Alm, (503) 947-5255

### Privacy Coordinators

Linda Weight

CAF/Field Services, (503) 945-6119

Gloria Anderson

CAF/Child Welfare, (503) 945-5700

Ronald Barcikowski

CAF/OVRS, (503) 945-6734

Donna Weaver

SPD/Field Services, (503) 945-5977

Marilee Bell

SPD/DD, (503) 947-5262

Diane Duncan

OMHAS, (503) 945-6083

Steve Modesitt

Public Health, (971) 673-1293

Maynard Hammer

State Hospitals, (503) 945-2866

Terry L. Grover

Health/OMAP, (503) 945-6536

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540



## “Everybody Out of the Building!” - A Real Life Business Continuity Event

It's an average working day, and you're attending a mid-morning meeting and forging your way through the agenda items when staff members begin to complain that their eyes are watering. Soon after that, some people in the office begin to have difficulty breathing. Before long, the order is issued for the building to be closed and for everyone to be evacuated...and then what?

This was the dilemma faced earlier this summer at a state-owned building in Pendleton that houses

several different state offices and two DHS programs. A re-roofing project had gone on there for several months, but on this particular day, fumes from the boiling tar used in that project entered the building necessitating its closure. Temperatures in the mid-to-high 90s and very still air conditions on that day probably contributed to the event.

SDA-12 Manager, Kim Carnine made the call to close the first two floors of the building, which housed the DHS-CAF programs for Self-

Sufficiency and Child Welfare. State offices for DEQ, ODOT, Building Codes and the Department of Revenue on the third floor followed her recommendation. Once she'd ensured that all her staff were safely out of the building, Kim faced the scenario that Business Continuity Planners have termed, “Work site unavailable.”

How do you carry out the work of your program when the office location, the client files, the

*“CONTINUITY” cont. page 4...*

## Risks Associated with Internet Browsing

Earlier this summer a security incident was discovered at Oregon's Department of Revenue. It was caused by an employee's having accessed an illicit Web site and downloaded data-capturing “spyware.”

As a result of that incident, more than 1,300 people in Oregon were placed at risk of identity theft. DHS asks that all staff be aware of the following risks from spyware that can compromise data:

1 Computers can be infected with a virus or spyware simply by viewing an infected Web page or by opening an infected file. These malicious programs can be installed without the knowledge or consent of the end-user and can compromise confidential data.

2 Illicit sites (e.g., electronic game Web sites, pornographic Web sites, non-business-case related chat rooms) are often visited by mistake because they have names similar to legitimate sites or the user is directed there without their consent.

If this happens, the incident should be reported immediately to the DHS Information Security Office (ISO) to ensure that the computer is checked for infection. Failure to have the computer examined can result in the spread of the virus or spyware and can put DHS data and systems at further risk.

Spyware is software that covertly installs itself onto a computer and collects data such as passwords and other confidential information (In the incident at the Department of Revenue, the confidential data

consisted of Social Security numbers, names and addresses). Spyware installation can often be done without any visible symptoms. The only way to detect it is to have the system scanned with anti-virus software.

If any of the incidents listed below should occur, DHS requires that they be immediately reported to ISO in order for protective actions to be taken as soon as possible:

- An illicit Web site is mistakenly viewed on a DHS workstation
- An unusual number of “pop-ups” display during Web-browsing
- Any security warning is displayed or anything suspicious occurs while browsing the Internet
- Any symptom appears that may indicate the system is infected with a virus or spyware

.....  
"CONTINUITY" continued...

telephone system, and the computer systems that you usually rely upon are unavailable to you? And who knows how long that circumstance might last?

Fortunately for the people working at SDA-12 and for the clients they serve, this was a short-term closure (The problem occurred on a Friday and by the following Monday they were able to resume business at that site). In the absence of an alternative place to work, most DHS staff were sent home for the day.

"Key 'lessons learned' for us from that event revolved around communications," said Kim, who has managed that location for eight years. "On the positive side, we had good mechanisms for letting staff persons know what was going on as things changed."

As for similar events in the future, Kim noted, "We need to do a better job of educating people about the options available to us." She explained, "There are other state offices in the area that could temporarily house state workers, but we will need to have decided among ourselves which programs will go where and what resources we'll need to have in order to provide our services. Also, we need to make plans for how we'll access our Information Technology systems and we need to be familiar with those plans in order to know how to carry them out."

The DHS-Information Security Office (ISO) is coordinating the Business Continuity Management program for Oregon's Department of Human Services. ISO staff will be meeting with representatives from each DHS division (e.g., CAF, SPD, HS, AS) in September and October.

The goals of those meetings will be to assist those divisions in determining their next steps in continuity planning. This will include identifying key teams (e.g., for planning, incident management, damage assessment, etc.), identifying tool users (i.e., individuals who will develop, test and update plans electronically) and identifying plan managers for each division.

If you have questions about Business Continuity Management within your division, the following persons have served as DHS Business Continuity Planning Coordinators for their divisions:

Administrative Services-Linda Riddell (Facilities), Dennis Wells (OIS), Julie Davie (HR) Kelli Heflin & Richard Templeton (ISO), CAF- Leona Gildersleeve, Health Services- Dusty Charters (OSH), Steve Modesitt (Public Health), Cherri Kietzmann (OMAP), Robert Furlow (OMHAS & BMRC), Bob Clabby and Donna Weaver (SPD).

In addition to these coordinators, the following DHS personnel have been participating in the DAS-

sponsored Business Continuity Planning Academy (a 10-day training on BCP terminology, planning steps, strategies, techniques and tools):

Gail Ault (SDA-12), Conrad Bozlee (SPD-State Operated Community Programs), Kelli Heflin (ISO), Steve Modesitt (PH), Nan Newell (Public Health Preparedness), Nick Reed (EOTC & BMRC) and Jennifer Staatz (SDA-7).

For additional questions on Business Continuity within DHS, Patty McCary is the program manager for Business Continuity Management in the Information Security Office.

You can also visit ISO's Web site at <http://egov.oregon.gov/DHS/admin/infosec/index.shtml> or send us an email at [dhsinfo.security@state.or.us](mailto:dhsinfo.security@state.or.us).

**ANSWERS  
to questions  
from page 2:**

- 1 - a.**
- 2 - b.**
- 3 - b.**
- 4 - a.**
- 5 - a.**
- 6 - a.**
- 7 - b.**
- 8 - a.**
- 9 - a.**

**The information provided in the Privacy/Security Update is intended for employees of the Oregon Department of Human Services. It is not intended as advice, legal or other, to any entity outside of the Department.**