

**Information Security Office
Communication, Education & Awareness Plan**

August 05 – July 06



A complete listing of all DHS Information Security Office information can be found at:

<http://www.oregon.gov/DHS/admin/infosec/>

For more information about this plan, contact:

Trish Neiworth,
DHS Communications
Public Affairs Office
(503)-945-5922
trish.neiworth@state.or.us

If you have a disability and need this publication in an alternate format, contact DHS Public Affairs Office at: 503-947-5107

Contents

Communication objectives.....

Key messages.....

Milestones.....

Target audiences.....

Communication
processes.....

Strategies.....

Communication Tactics

1. All Audiences
2. Internal Audiences: All DHS Employees
3. Internal Audiences: Targeted Mangers, Staff, Committees
4. Combined Communications: Web sites
5. External Communications: Stakeholders
6. External Communications: Public/Media
7. Internal Staff Support

Situational Analysis & Risk Factors

Appendix A: Email Decision Tree

Communication Objectives

What ISO must communicate

The Information Security Office (ISO) must communicate about the confidentiality, integrity and availability of DHS information assets. The ISO must communicate the following:

- What staff are required to do by law.
- Areas where security & privacy policies, procedures and controls are in alignment with federal and state regulations and industry best practices.
- How ISO will apply a level of security to information resources commensurate to their value to the organization, and sufficient to contain risk to an acceptable level.
- Program and service delivery responsibilities for successfully implementing privacy and security measures in DHS program and service processes.
- Ramifications staff may face if they breach security and privacy policies.

Education & Awareness around needed staff Behavior Changes

The ISO must identify and facilitate staff behavior changes in order to move the organization into a secure environment. The communication program must also include education and training for key areas identified by the ISO. Those key areas include staff behavior changes, compliance with rules, and ensuring the stability of the security system as a whole within the department.

All audiences

- Communicate what law requires.
- Communicate changes the department is making around the confidentiality, integrity and availability of information assets.
- Communicate ramifications/consequences for breaches in the areas of confidentiality, integrity and availability for information assets.

Internal audiences

- Communicate policies, procedures and key dates that impact staff.
- Educate staff on behavior changes they need to make in order for the department to be compliant with rules & policies.
- Educate staff on behavior changes they need to make in order to reduce the risks of security, privacy incidents.

External audiences

- Communicate changes in policies and procedures that impact them.
- Communicate what DHS is doing to meet national rules and other related regulations or audit findings.

Key messages

Messages will be part of the daily work of all ISO employees and will help to guide the work that needs to be accomplished. Key messages are an overall focus for the work that needs to be accomplished in the next year; additional detailed information may need to be shared as a part of these key messages.

Responsibility: Keeping confidential and sensitive information secure and private is everyone's responsibility.

Definitions: Information Security means protecting all forms of confidential and sensitive information. (*Computers, Copies, Conversations*)

Privacy is an individual's right to keep personal information protected and to determine who should have access.

Requirements: DHS is required by law to prevent, detect, contain, report and correct information security and privacy incidents.

Expectations: All DHS staff members must ensure our clients', employees' and partners' information is protected and available because it is our obligation to do so.

Integration: Information Security and privacy will promote program integration in a secure environment.

Communication Milestones

(Bolded areas indicate communication & education/awareness needs because of required staff behavior changes.)

September 2005

- Privacy/Security Newsletter

October 2005

- SAT

November 2005

- Privacy/Security Newsletter
- **Policy Communication (Access Control)**
- **Secure e-mail**

December 2005

- **Secure e-mail**

January 2006

- Privacy/Security Newsletter
- CNIC
- **PSIRP**
- **Misdirected email**

February 2006

- Business Continuity Planning
- **Access Control**
- **Computer Based Training**

March 2006

- **BCP Project Update**

05-07

- Privacy/Security Newsletter

April 2006

- (Begin work on 2006-2007 Communication Plan)
- Business Continuity Planning
- **Policy Communication (Information Security Program)**

May 2006

- Privacy/Security Newsletter

June 2006

- Business Continuity Planning

July 2006

- 2006-2007 Communication Plan Finalized
- Privacy/Security Newsletter

Target audiences

Identified *internal* target audiences include:

- DHS Managers/Supervisors
- DHS Exec Teams
- DHS Field Services & Programs
- IT Staff (OIS)
- DHS Trainers
- Public Health
- OSH/Group Homes - Hospital
- DHS Cabinet
- Chief DHS Data Stewards
- DHS Business experts (CAF & SPD)
- All DHS Staff
- Volunteers

Identified *external* target audiences include:

- Labor Representative
- Stakeholders
- Contractors/Providers
- Legislators
- Other State Agencies
- County Partners
- General Public/Media
- DHS Clients
- Federal Partners
- DAS
- Boards, Commissions, Councils

Communication process

Methods

The primary methods used to disseminate information and/or educate for behavior changes:

Electronic communication

This includes but is not limited to such communication vehicles as targeted emails, web sites, Privacy/Security newsletter, internal mail lists, DAS electronic communications, Director's Message, DHS Staff News, OIS Wednesday Messages, email clearinghouses and other means of rapid information dissemination. The key hub for the Oregon DHS ISO web site is http://www.dhs.state.or.us/admin/info_security/. This web site will provide access to the office's progress and activities and will be updated regularly. Once the DHS Intranet site is operational, that will be used for "staff only" types of communication, forms and procedures.

Printed communication

This includes printed or copied documents as needed to fulfill the communications objectives. These include talking points, fact sheets, program newsletters, news releases, newsletter articles for partner and association newsletter, progress reports, brochures, training materials, booklets and other items as necessary.

Verbal (Training) communication

This includes speaking engagements, presentations, and formal training classes in a variety of forms including classroom style, videotaped, videoconferencing and computer based training and computer conference style education. Meetings may include executive level briefings, team briefings, office or unit staff meetings, customer meetings, partner meetings, provider meetings and stakeholder briefings.

Visual communication

Often this will include materials to be used in presentations, speaking, or training. These include PowerPoints, videotapes, and other visual charts, graphs, posters and pictures.

Strategies

ISO communication strategies will be multi-faceted and carried out using a variety of communication methods. Key strategies include:

- **Information Only:** Determine if the communication is “information only.” Once determined, that will drive the types of communication methods needed – relying more on utilizing the traditional electronic communications channels (Email, email newsletters – Staff News, established messages – OIS Wednesday message, Director’s Message, etc.)
- **Seeking Behavior Change:** Determine if the communication is seeking “a staff behavior change.” If so, the means of communicating that information is more complex and should involve actively engaging staff either through a task, class or activity. This is to ensure that the behavior change is acknowledged and recognized.
- **Managers as Key Communicators:** Rely on management at all levels to help communicate key messages and behavior changes. Develop a matrix of which levels to use for which type of information. It will be critical to be strategic on who, how, and how often these managers will be used to help carry messages. Too much repetition of this method will lead to dilution of messages; whereas no use of managers at various levels will not allow necessary buy-in.
- **Getting Staff’s Attention:** Rely on various staff meetings to help communicate critical behavior changes. In order to get staff’s attention on major changes, they need to hear it from their own managers in their own meetings.
- **Behavior Changes –Three Ways for real learning to occur:** For each behavior change needed, the strategy would be to offer staff and others the information three different ways in order for them to really “get it.” If possible these should include written (electronic/printed); visual of some sort and/or hands-on activity (entering their new password for example), and audio (verbal). Because of the volume of information shared with DHS staff and others daily, it is clear that without a combined strategy on the key behavior changes staff will have trouble absorbing, remembering, or even making the needed changes.

Communication tactics

1. Information Security Awareness – All Audiences

A. Information Security/Privacy Officer Interaction

Meet with peers and customers on a regularly scheduled basis. (At least quarterly i.e., SDA managers, AAA's). Track questions and follow up issues.

Due Date: Ongoing
Responsibility: ISO Privacy and Security Officers

B. Develop Fact Sheets on Critical Issues

Develop fact sheets to be used with external audiences on critical ISO issues. These will be developed on an as needed basis.

Due Date: TBD
Point Person: Program Manager

Business Continuity Planning
Access Control
DHS Privacy Program
Information Security
Incident Response

C. Document review

Review and make suggestions for improvements to key project and or program documents, but not correspondence, as defined:

- Anything that will end up on the Web site
- Legislative Committee materials
- Key Presentation materials
- Anything representing an official position on the project or program; including reports to DAS, etc.

Due Date: As needed
Responsibility: OPA

Communication Tactics

2. Internal communications: All DHS Employees

A. Director's message

At least each quarter, at the Director's discretion, include information that reinforces the importance of the ISO work and what it means to clients and staff to help them understand how it affects them.

Due Date: As needed

Responsibility: Program Manager/OPA

B. DHS cabinet

Periodic updates to cabinet to include activity reports, budget status, benefits to DHS of work to date and future activities. Communication needs to achieve continued financial and staff resource commitment from DHS Cabinet.

Due Date: As needed

Responsibility: Program Manager/ISO Security Officer/Privacy Officer

C. DHS Staff News

Periodic articles provided to DHS Staff News (electronic employee newsletter) on featured IS activities.

Due Date: Ongoing

Responsibility: ISO Team

D. Information Security Alert

Email that goes out immediately because of severity of the issue. (See attached email communication decision tree: Appendix A.)

Due Date: As needed

Responsibility: Program Manager/OPA

E. Privacy/Information Security Newsletter" Update"

Electronic newsletter provided every other month to staff and others on key Privacy and ISO issues.

Due Date: Bi-Monthly

Responsibility: Privacy Officer/A&E Program Manager

F. Staff Feedback loop

Maintain and publicize a staff feedback loop (Information Security Privacy Email) where questions can be posed and answered. Via monthly ISO email message or other means. Track questions/answers.

Due Date: Completed

Responsibility: Privacy Officer/ISO Program Manager

G. Change Control Communications

Develop process for communication around “change control” issues – i.e., when software upgrades are occurring and there is a need for communicating on those. Work with Strategic Applications section and others on communication needs around these processes.

Due Date: TBD

Responsibility: Security Analyst

Communication tactics

3. Internal communications: Targeted Managers/Staff/Committees

A. Manager Meetings

Meet as needed with managers or department-wide committees to share important information. Identify issues that they need to communicate. Send critical reminders and info to managers pertaining to ISO issues on an as needed basis.

Due date: On-going

Responsibility: ISO Program Manager– Point Person; Topic related/ISO Lead

B. ISO Manager Action Requests

Send critical reminders and info to DHS managers on ISO issues as needed.

Due Date: Ongoing

Responsibility: Privacy Officer - Point Person; Topic related/ISO Lead

Communication tactics

4. Combined communications: (For internal and external Use) – Web site

A. Overall use of DHS ISO Internet Web site

This should be the hub of all ISO communications, except for those “staff only” types of communications and forms. Continue to make site more robust, weekly postings.

Due Date: Ongoing

Responsibility: A&E Program Manager and ISO Webmaster

C. Other ISO-related documents

Post other ISO related documents that are public documents including those from various sections, projects and initiatives.

Due Date: On-going

Responsibility: A&E Program Manager and ISO Webmaster

Communication tactics

5. External Communications: Stakeholders

A. Stakeholder presentations

Present ISO updates in formal meetings of organizations such as the Conference of Local Health Officials, Governor's Commission on Senior Services and others and to official DHS advisory bodies. Determine stakeholder groups applicable, build schedule.

Due Date: Ongoing

Responsibility: ISO Security & Privacy Officers/ Program Manager

Data Base Recording: OS2

B. Communication with other State Government Agencies/DAS

Identify a point of contact for other state government agencies on ISO issues. Share successes on a regular basis; also good way to determine barometer on new ideas, approaches.

Due Date: Ongoing

Responsibility: ISO Security Officer & Privacy Officers/Project Lead

C. Statewide Conference Participation

Participate in statewide conferences, symposiums, and summits as set by the department.

Due Date: Ongoing

Responsibility: ISO Security & Privacy Officers Officer/A&E Program Manager

Communication tactics

6. External communications: Public/media

A. ISO-related news releases

Work with Public Affairs Office on any news release that may be needed.

Due Date: Ongoing

Responsibility: OPA

B. ISO fact sheets

Create fact sheets on initiatives or projects as needed for use with the public and/or news media.

(See Tactic 1D)

Due Date: Ongoing

Responsibility: OPA

C. Media Response

Be available to respond to media inquiries relating to ISO as needed.

Due Date: Ongoing

Responsibility: OPA

D. Legislative/congressional response

Be available to respond to legislative and congressional inquiries relating to ISO as needed.

Due Date: August 2004

Responsibility: DHS Legislative Coordinator in coordination with ISO team

Communication tactics

7. ISO staff support

A. Project/Initiatives Kick-Offs

All projects should have some sort of tasks and schedule built in to the work to be accomplished that include some kind of kick-off or launch and some communication elements. Work with ISO Communication Specialist/Public Affairs on building these activities into project schedules.

Due Date: Ongoing

Responsibility: ISO Program Manager, Point person: Project Manager

B. ISO Budget and related presentations

ISO should have a budget presentation completed prior to the legislative session, as directed by the Director's Office. Other special presentations may be needed from time to time depending on the initiative or project. Support from ISO Communications Specialist/Public Affairs on review of these key external documents and assistance, if needed, in editing and adding value.

Due Date: TBD

Responsibility: ISO Program Manager

C. Media/Legislative Speaker's Training

Make training available to media/legislative spokespersons. Offer practice sessions on controversial subjects.

Due Date: TBD

Responsibility: OPA

Situation Analysis

This situation analysis was designed to identify issues that would affect the types and methods of communication needed to help the department be successful in this effort. This is a compilation of information provided by the Information Security Office.

Overview

Today's complex information age can provide DHS with large quantities of data after a few seconds at the computer keyboard. This deluge of information also presents the department with security challenges as never before in history. Securing information means protecting all forms of confidential and sensitive information. This is not limited to information on computers, but oral and paper information is equally as important.

Protecting information ensures its availability, integrity and confidentiality. Protecting sensitive information preserves everyone's privacy. It protects our clients, our staff, our partners, and Oregon citizens. DHS handles a high volume of confidential medical, financial and client information that can be misused through security breaches.

DHS is working on three key changes to improve its security:

- Policies and procedures around who has access to information and who it can be shared with.
- Technology-based safeguards such as stricter requirements for passwords and strengthening the network.
- Physical safeguards, such as locking file cabinets and keeping confidential papers out of view.

Risk Factors

Staff Ownership

All staff in the department are responsible and legally required to keep confidential information safe and secure. The law requires that we must all protect client and employee confidential information and data. Information security is not an option. There are a number of driving forces including HIPAA Privacy and Security rules, federal and state laws and regulations, the Secretary of State and internal audit findings and identified security risks through assessments. Our systems will not be secure through technology improvements alone. The information assets that DHS holds will be protected only if all employees participate.

Multiple Communication Channels

There is no single method to communicate with customers, providers, staff or clients, so multiple methods will be needed.

Relationships with other organizations, counties, stakeholders, partners

Relationships differ throughout the department with counties, stakeholders and others. The level and means of communication also varies throughout the department. One risk factor is that individuals could be missed if communicators are not fully aware of how each part of the department and its stakeholders are reached (or not reached) depending on the situation.

Stakeholder, provider and partner mailing lists exist throughout the department in various levels and forms. There is no plan at this time to consolidate these various lists; thus a splintering occurs in how communications are transmitted. This needs to be recognized and acknowledged as a risk factor. Any improvement in this overall external communication means would have a staffing impact.

I:\Information Security\A&E\Richard's\FINAL 05-06 ISOCCommPlan.doc

Appendix A: All Staff Email Communication - Decision Tree for DHS Information Security Office

When information needs to go out to all DHS staff or a target audience, three options are available:

1. Security Alert Communication (for those that need to be made the same day because of a serious emergency situation);
2. Security Watch (which asks staff to either change a practice or warns them of an impending threat); and
3. Privacy/Security Newsletter (which goes out every other month and includes general information on privacy and security issues, updates to previous information, or other purely informational privacy and security items.)

Information Security Alert

Email Goes out Immediately

(Meets at least 1 Alert Criteria)

- Issue could immediately shut down network (*Develop emergency communication method if network is shut down.*)
- Issue could freeze computer
- Issue could immediately stop work at DHS
- Issue poses immediate health/safety risk
- Issue poses immediate risk of exposure to confidential information

Check Points:

- Draft is reviewed and edited by Business Security Manager
- Appropriate target audience is determined; all staff, managers, etc.
- Draft is reviewed by the Public Affairs Rep (if possible)
- Final draft must be reviewed and approved by the ISO Program Manager and/or Information Security/Privacy Officer prior to transmittal.

Privacy/Information Security Watch

Email goes out when needed

(Meets at least 1 Action Criteria)

- Staff need to be aware of a potential danger to information systems, (viruses, etc)
- Staff need to be aware of a potential information security/privacy threat (scams, disclosures, etc)
- Action is needed by staff to change current practices to improve security
- Action is needed by staff to start new practices to improve security

Check Points:

- Draft articles are submitted by the deadline to the Business Security Manager
- Articles are reviewed, edited and included in one email message
- Draft message is reviewed by the Public Affairs Rep and ISO staff
- Final draft must be reviewed and approved by the ISO Program Manager and/or Information Security/Privacy Officer prior to transmittal.

Privacy/Info Security Newsletter

Email goes out every other month

(Meets Informational Criteria)

- Information about ISO
- General security/privacy info
- Tips or other tools available
- Links to more information/resources
- Additional information addressing recent security alerts or security watch topics

Check Points:

- Draft Privacy articles must be submitted by the deadline to the Privacy Officer
- Draft Security articles must be submitted by the deadline to the Awareness and Education Manager
- Articles are reviewed and edited by the Privacy Review and A & E Teams
- Final draft newsletters are shared with the Public Affairs Rep and ISO staff
- Final draft must be reviewed and approved by the ISO Program Manager and/or Information Security/Privacy Officer prior to transmittal.