Double-click here for an accessible version of this document:

VOLUME 1, ISSUE 3

THE NIH EYE ON PRIVACY

MAY 2008

OFFICE OF THE SENIOR OFFICIAL FOR PRIVACY

INSIDE THIS ISSUE

CALENDAR OF EVENTS

PIA Training
May 7, 23 and June 6
10401 Fernwood Rd.
Lower Level Classroom
Room 1NW-02
Bethesda, MD 20817

CIT Online Training:
http://training.cit.nih.gov
Keyword Search: PIA

Privacy Coordinator Group Meeting:
May 28, 9:30–11:30 a.m.
Executive Plaza (EPN)
Conference Room G

HHS Computer Security and Privacy Awareness Day
June 3, 2008
Hubert H. Humphrey Building, 9–11 a.m.

Program Support Center (PSC) Parklawn Building
1–3 p.m.

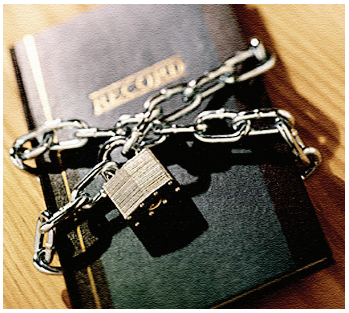
PRIVACY PRACTICE: NIH PRIVACY AWARENESS TRAINING LAUNCH

By June 30th, 2008, employees must complete annual NIH Information Security Awareness Training. Beginning this year, NIH Privacy Awareness Training will be introduced as a new requirement. It is live now and can be viewed by logging in to http://irtsectraining.nih.gov. Although the course is not yet mandatory, you are welcome to take it. An administrative back-end to the training course will allow us to track user completion and will provide you with a certification of completion upon successful completion of all course modules.

Over the next few months, we will roll NIH Privacy Awareness Training out to employees and contractors in two phases. As part of the initial phase of the release, those designated by the NIH Executive Officers as having a "significant" role with respect to privacy will be contacted next month and asked to complete the course by a specified deadline. These are a) individuals who are involved in the design, development, operation, use, or maintenance of any record in a Privacy Act System of Records, b) agency personnel and contractors with access to federal data; and c) individuals, including contractor personnel, directly involved in the administration of personal information or IT systems, or with significant information security responsibilities.

The second phase will mark the release of training to all remaining employees and contractors. Moving forward, all employees will be required to complete training within 60 days of employment, and annually thereafter. More communication will be sent to inform you of the status of the requirement and announcements will be made in the NIH Record.

The completion of NIH Privacy Awareness Training is important to us all. We need to be aware of the potential privacy and security risks associated with the work that we do. Understanding the risks to the privacy of the data we are obliged to protect and the security of the IT systems used to manage that data requires personal "buy in". Only when we embrace privacy and security will secure means of communication, encryption and passwords do their job. NIH Information Security & Privacy Awareness Training will help us to become more aware of the sensitivity of the personally identifiable information that we collect, use, store, and disseminate, and educate us to do a better job to protect it.



Karen Plá
NIH Senior Official for Privacy

HHS COMPUTER SECURITY AND PRIVACY AWARENESS DAY

On Tuesday, June 3, 2008, Secure One HHS is sponsoring its third annual HHS Computer Security and Privacy Awareness Day entitled "Cyber Strength: Condition Yourself for Protection". Come and learn about computer security and privacy threats and how to keep you and your family safe. This is one event that you do not want to miss!

The event will be held at two locations:

- Hubert H. Humphrey Building, 9–11 a.m.
- Program Support Center (PSC) Parklawn Building, 1–3 p.m.

A web cast of the event will also be available at http://videocast.nih.gov.

Participation is free and all HHS employees are encouraged to attend.

TRAINING: PRIVACY IMPACT ASSESSMENTS

Calling all IT System Owners/Managers, IC Privacy Coordinators, ISSOs, IT Administrators (networks, servers, databases), Webmasters/Administrators, OMB Project Clearance Liaisons and other NIH staff involved in the Privacy Impact Assessment (PIA) process! Do you know about the responsibility to complete PIAs for all NIH IT systems? Are you new to NIH? Join us for training that will be offered in the coming weeks on conducting PIAs on IT systems. *Completion of Privacy Impact Assessments (PIAs) Using the HHS Security and Privacy Online Reporting Tool (SPORT)* will provide an overview of the HHS requirement to conduct a PIA on IT systems, how to access and use the online reporting tool called SPORT, and how to complete a PIA. This will be an informative opportunity to ask questions related to PIAs and NIH privacy requirements, and network with others across NIH with similar responsibilities. For dates and locations, please see the Calendar of Events on Page 1.

NIH Office of Management Assessment

6011 Executive Blvd., Suite 601
Phone: (301) 451-3426
Fax: (301) 402-0169
Email: privacy@mail.nih.gov

The Office of the Senior Official for Privacy serves as the chief NIH privacy governance entity whose mission is to ensure the highest level of scientific integrity, public accountability, and social responsibility in the area of privacy management.

For more information about the OSOP, the Privacy Act, PIAs and privacy at NIH, please visit us at: http://oma.od.nih.gov/ms/privacy
To obtain more information about IT security at NIH, please visit: http://www.cit.nih.gov/security.html

VOLUME 1, ISSUE 3

THE NIH EYE ON PRIVACY

MAY 2008 OFFICE OF THE SENIOR OFFICIAL FOR PRIVACY

Privacy Points of Contact

Find contact information for NIH IC Privacy Coordinators at the following site: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3

SPOTLIGHT ON OMB MEMOS

This month we focus on OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." OMB mandates that agencies must reduce or eliminate its use of social security numbers. Agencies must now review their use of SSNs in agency systems and programs to identify instances in which collection or use of it is superfluous. We should always be mindful of where and why we are using SSNs. Ask yourself: Is the SSN necessary to fulfill the NIH mission? Can you accomplish your work without it? This memo has particular relevance as a result of the recent NIH laptop theft. In order to protect our staff and the public, we must continue to assess whether the collection and storage of SSNs is critical to our research initiatives and, if not, work to reduce or eliminate the use of them. Those who wish to review the memo and its mandates can visit: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

We are on the web!

http://oma.od.nih.gov/ms/privacy

IN THE NEWS

All About the IRS Rebate Numbering System

San Francisco Chronicle | Kathleen Pender | Tuesday, May 6, 2008

The Internal Revenue Service's decision to distribute economic stimulus payments based on the last two digits of your Social Security number got me wondering: How does the government assign these numbers? Is there anything you can tell about a person from his or her number? And in using the last two digits, is the IRS favoring one group over another?

It turns out that the first three digits—called the area number—are based on the ZIP code of the mailing address listed on the application for a Social Security number. It can usually tell you something about a person's origins.

Within each area, the next two digits—called the group number—are assigned in consecutive order as applications come in. Instead of going from 01 to 99, however, the Social Security Administration follows an odd-even numbering pattern. Within each group, the last four digits are assigned in consecutive order from 1 through 9999. Read More: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/05/06/BUCS10H2DD.DTL

ISSO CORNER: I FORGOT MY PASSWORD

I keep forgetting my password. What can I do?

Take a few minutes now and register at http://iForgotMyPW.nih.gov and your solution will be only a few clicks away.

Did You Know?

More than 162 million records were reported lost or stolen in 2007. According to USA TODAY's analysis of data losses reported over the past two years, that's triple the 49.7 million that went missing in 2006.

How do I register? Simply go to http://iForgotMyPW.nih.gov and validate your NIH account. In order to register, you will be asked to provide five unique answers to five questions. When you need to reset your password, you must correctly provide three of those registered answers. If you have not registered and you do not know your password, you must contact the NIH Help Desk for assistance at (301) 496-4357, (866) 319-4357, or Toll Free at (301) 496-8294 (TTY).

Are there other benefits for registering?

When you are not able to access the iForgotMyPW site to reset your password, but you are registered there, the NIH Help Desk can assist! For security reasons they are required to perform basic "identity proofing" and are authorized to ask the key questions. Upon receiving three correct responses, they can quickly change your password for you.

If you need to reset your other non-active directory passwords, you can use your NIH Password to log in at Password Reset (http://silk.nih.gov/passwordset) where NIH users can reset their Helix, ALW, and Titan passwords.

How do I reset or unlock my account once I have registered?

Go to http://iForgotMyPW.nih.gov, validate your account, and then select the function you need from the menu. It's that simple!

DEPARTMENT OF HEALTH & HUMAN SERVICES • USA

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health