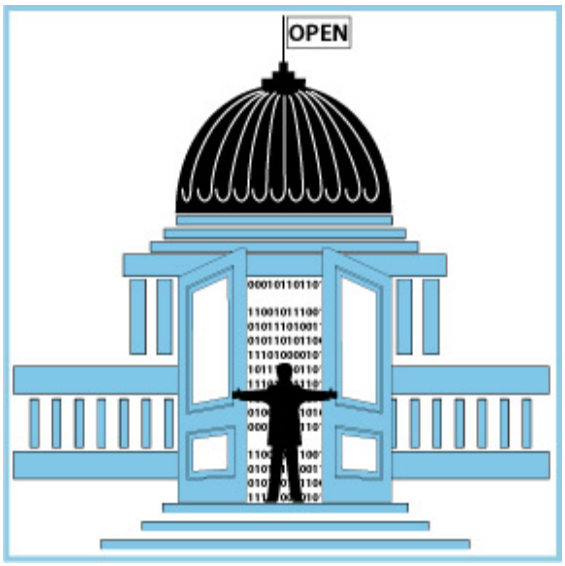
INTERFACE Online
Published by the Center for Information Technology, National Institutes of Health

Winter 2009 [Number 245]



Major Articles

Published By
Center for Information Technology
National Institutes of Health
Health and Human Services

Table of Contents

Articles

http://www.nih.gov is one of the most frequently visited federal government websites.

	July	*August*	*September*
Total hits for the month	65,524,011	63,928,636	68,968,732
Hits per day	2,113,677	2,062,214	2,298,957
Different individuals per month	3,041,488	3,054,816	3,089,744

The server has been up 100% of the time* during November 2009.
** Server uptime is independent of network accessibility.*

Articles

Open Identity for Open Government at NIH

For over a year now, NIH has been employing Federated Identity Management to provide staff with the means to collaborate with colleagues from outside NIH, including those from universities, other Department of Health and Human Services (HHS) Operating Divisions, and other federal agencies. For this purpose, CIT created the NIH Federated Identity Service.

NIH Federated Identity Service (the basics)

The NIH Federated Identity Service allows authorized individuals to access multiple applications and data sources across agencies using a single login and password. The service was featured in issue #243 of *Interface*, which explained how Federated Identity Management works, the role of the NIH Federated Identity Service in providing authorized users with access to resources, the benefits for individuals and agencies of using the service, and how security issues are addressed. The bottom line is that users save time and have easier access to resources, NIH reduces IT expenses because there are fewer outside accounts and help desk calls, and security is improved since the likelihood of logins and passwords being compromised due to "password overload" is lessened.

Until now, this service has been available only to researchers and other users at partner agencies and higher education institutions through the InCommon Federation, an education/industry/government consortium. If your agency or university did not have a Federated Identity Management agreement through InCommon, or if you were a private citizen without institutional affiliation, you were out of luck, and could only access NIH resources the old-fashioned way—a separate login and password for each application or resource.

Expanding access

This is changing in a big way. On September 9, 2009, ten industry leaders—Yahoo!, PayPal, Google, Equifax, AOL, VeriSign, Acxiom, Citi, Privo, and Wave Systems—announced that they will support the first government Open Identification pilot program. These companies, using OpenID and Information Card technologies, will act as digital identity providers. The federal-wide Open Identity for Open Government Initiative seeks to work towards making it easy for individuals to register and participate in government websites without having to continually create new usernames and passwords — a goal set in President Obama's January 2009 Transparency and Open Government memorandum.

Dr. Jack Jones, NIH CIO and acting director, CIT, announced: "As a world leader in science and research, NIH is pleased to participate in this next step for promoting collaboration among agencies and institutions. Within a few weeks, OpenID and Information Card credentials will join those currently in use from InCommon as external credentials trusted by NIH."

The Open Identity for Open Government Initiative

The intent of the initiative is to transform government websites into more accessible and interactive resources, saving individuals time and increasing their direct involvement in governmental decision-making. NIH is the first federal agency to participate in the Open Identity for Open Government

Initiative pilot program. The ten participating companies are being certified under non-discriminatory open-trust frameworks developed under collaboration between the OpenID Foundation (OIDF) and the Information Card Foundation (ICF) and reviewed by the federal government.

OpenID and Information Card technologies make such access simple and safe. For example, in the coming months NIH intends to use OpenID and Information Cards to support a number of services including customized library searches, access to training resources, registration for conferences, and use of medical research wikis, all with strong privacy protections. "This is a significant leap in participatory democracy," said Don Thibeau, executive director of the OpenID Foundation (OIDF). "Following President Obama's directive, our government has worked with market leading companies to leverage modern, open standards to engage with its citizens. When the government adopts open identity standards and trust frameworks, the result is better service, more transparency, and greater accountability."

OpenID and Information Cards

OpenID is a web registration and single sign-on protocol that lets users register and login to OpenID-enabled websites using their own choice of OpenID identifier. With OpenID, individuals can use the services of a third-party OpenID provider (such as AOL, Google, or Yahoo), where they may already have an account. One key advantage of OpenID is that it requires no client-side software—it works with any standard Internet browser.

An **Information Card**—often described as a "virtual wallet"—is a new approach to Internet-scale digital identity in which all of a user's identities, whether self-created or from third party identity providers (such as an employer, financial institution, school, or government agency), are uniformly represented as visual "cards" in a software application called a card selector. There are three types of cards: personal (self asserted), managed (issued by a 3rd party) and mixed (3rd party with additional self-asserted information).

Both standards can provide different Levels of Assurance (LOAs) in regard to verifying the identity of the user. For some activities, such as saving library catalog searches, these credentials will enable the user to remain completely anonymous; for others they may require personal information such as name, email address, age, gender, and so on. The Open Identity for Open Government Initiative will enable individuals to choose the identity technology, identity provider, and security credential with which they are most comfortable, while enabling government websites to accept and trust these credentials. This approach leads to increased innovation and lower costs for both government and citizens.

Open trust frameworks also allow different levels of trust based upon what the organization decides is needed by particular individuals. No matter which standard is utilized, authenticated users have access only to those resources for which they have been authorized. "Open government cannot and will not compromise either security or privacy," said Drummond Reed, executive director of the Information Card Foundation (ICF). "By working with private industry, the U.S. government is harnessing the innovation and efficiencies of the open market and letting citizens choose their preferred means of engaging with government agencies."

Benefits for the average user

What will these developments do for the average user—the researcher at the National Cancer Institute, the Food and Drug Administration (FDA) grant reviewer, the graduate student at Ohio State studying dementia, or the private citizen doing a search on PubMed for a disease they are being treated for?

First, OpenID and Information card technology will allow all of these users access to NIH and related resources, even if their institution or agency does not have an agreement with the NIH Federated Identity Service, or if they are unaffiliated with any government agency or higher education institution. Likewise, NIH staff will be able to gain access to resources provided by organizations that are not affiliated with the service, as long as the resource they seek access to accepts OpenID or Information Card.

Second, these technologies will help safeguard user privacy and the security of the applications they use. For the user, this means that sensitive personal information (such as one's email address or login password) will not have to travel back and forth over the Internet for each login transaction. Using OpenID and Information Card protocols, authentication needs to be verified only once. Because users will need to remember only one login and password for numerous applications and resources they use, they will be less tempted to write down such sensitive information near their computer, potentially compromising access to confidential data.

Third, the plan is to expand the Open Identity initiative to agencies beyond NIH. The FDA is already taking part in the Federated Identity Service and will take part in the Open Identity initiative. GSA has signed on, and the Library of Congress has expressed a strong interest in joining.

Recognition

NIH/CIT first got involved in working on federated identity in 2006 with the creation of a Federated Authentication Initiative. Cross-team discussions and R&D culminated in the NIH Login to support federated identity in 2007 and the full implementation of the Federated Identity Service (NIH Federated Login) in 2008. This pioneering work in the field of identity management was recognized with the NIH Director's Award in 2008 for the Federated Authentication Initiative, which was led by Debbie Bucci, Valerie Wampler, Jane Small, Jim Seach, Tom Mason, and Peter Alterman.

The Government Information Technology Executive Council (GITEC) has awarded the GITEC 2009 Project Management Excellence Award to the NIH Federated Identity Service Team. Valerie Wampler accepted the award for Jack Jones, Debbie Bucci, and NIH/CIT at GITEC's annual Information Processing Interagency Conference in March 2009. The award recognized the contributions made in the field of federated identity by the NIH Federated identity Service.

The NIH Federated Authentication service was selected as one of the top 10 Government Innovators by *InformationWeek* 500.

Current status and future action

The Federal Identity Credential and Access Management subcommittee (FICAMSC) of the Chief Information Officers' Council has developed a Trust Framework Adoption Process for Levels of

Assurance (LOA) 1, 2, and 3 and a Scheme Adoption process to access credential providers. OpenID has established a scheme that currently qualifies at LOA1—the least stringent level of security, commonly used for blogs and other low-risk resources. NIH is currently testing OpenID with Google, Yahoo, VeriSign, and PayPal. Information Card has established a scheme that qualifies for LOA1, LOA2, and LOA3; PayPal and Equifax are proceeding with the adoption process to qualify at LOA2 and LOA3.

The OpenID Foundation (OIDF) and the Information Card Foundation (ICF) have adopted a common framework to certify identity providers. Under the OIDF and ICF's open-trust framework, any organization that meets the technical and operational requirements of the framework will be able to apply for certification as an identity provider. These organizations can then supply authentication credentials on behalf of their users.

Initially, the NIH SSO service will accept Open ID credentials as part of an "Open for Testing" phase. At that time, InCommon will begin to use OpenID and Information Card credentials. The NIH National Center for Biotechnology Information (NCBI) will implement OpenID for myncbi accounts, which support PubMed, and their SharePoint site for LOA1 resources. NIH Login will add Information Cards, as soon as upgrades are possible, for PayPal and Equifax. FISCAM is expected to endorse more stringent one-time password (OTP) technology from both the banking and wireless industries to support LOA3 applications.

End game at NIH and beyond

The end goal of the Open Identity for Open Government Initiative at NIH/CIT is to give users of NIH websites and other electronic resources the ability to have a single account and login procedure that will allow access to all NIH applications, as well as other government and private sector applications. This will make it easier for users to access information resources, remove the responsibility for security authentication from website and application owners, and improve security.

More information

You can find more information about Federated Identity Management at the NIH Federated Identity page (http://federatedidentity.nih.gov). For more information on NIH work with OpenID and Information Card protocols, please contact the NIH Help Desk at http://ithelpdesk.nih.gov or by phone at 301-496-4357, 301-496-8294 (TTY) or toll free at 866-319-4357 (toll free).

You can also find more about OpenId and Information Card at the following websites:

Open Identity Solutions for Open Government
http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV

OpenID/Information Card white paper "Open Trust Frameworks for Open Government"
http://wiki.informationcard.net/files/Open-Trust-Frameworks-for-Open-Gov-2009-08-10.pdf

OpenID Federation website
http://openid.net/

Information Card Federation website
http://informationcard.net/

Note: All direct quotes in this article are taken from the NIH/CIT Press release "YAHOO!, PAYPAL, GOOGLE, EQUIFAX, AOL, VERISIGN, ACXIOM, CITI, PRIVO, WAVE SYSTEMS PILOT OPEN IDENTITY FOR OPEN GOVERNMENT" (available here: http://cit.nih.gov/NR/rdonlyres/DF7C7DA9-3303-438F-BD3C-21D3859BB843/0/OpenIdentityInitiativeFINALRelease9909.doc).

An Announcement for *Interface* Print Subscribers

As of this issue, the printed version of *Interface* will no longer be sent out to subscribers. We encourage print subscribers who have not yet signed up for *Interface Online* to visit our home page at http://datacenter.cit.nih.gov/interface/ and subscribe to the listserv notification (via email) for *Interface Online*.

Reduce resource use

Since *Interface*'s first venture onto the Web in 1995, the focus of the publication has steadily shifted to its online presence. Most print publications have recognized the importance of presenting their content digitally, and the number of readers who expect to read articles online is growing steadily. With the switch from delivery by mail to email-only, *Interface* also supports NIH's Greening Goals (http://www.nems.nih.gov) of sustainability, energy conservation, and reduced consumption of natural resources like paper (see also *Interface* issue 240 for other greening efforts at CIT).

Interface listserv

Each new issue of *Interface Online* is announced through an email sent to listserv subscribers. If you are not already subscribed to the *Interface* listserv, simply follow these easy steps:

1. Go to the *Interface* home page at http://datacenter.cit.nih.gov/interface/
2. Click on Subscribe to *Interface* via Listserv located on the right-hand side of the page. This page allows you to subscribe/unsubscribe and also select your delivery options.
3. Sign up by entering an email address and your full name.
4. You will receive an email message with a confirmation code at the email address you provided. Once this message arrives, follow the instructions to confirm your subscription.

If you have a listserv password, you can login and update your subscription interactively, without email confirmation.

Questions?

If you have comments or questions about this change, please email *Interface* at interface@nih.gov — we are always happy to hear from you.

The Active Directory Manager (ADM)

Over the next several months, the Constellation account creation service (currently being used by some ICs) will be retired and Active Directory Manager (ADM) will become the enterprise provisioning service at NIH.

What is ADM?

The ADM service uses Quest's ActiveRoles Server software to provide a fully-featured tool for managing Microsoft's Active Directory (AD) accounts. ADM provides a single point of administration, delegation, policy enforcement, and change control for users, groups, and computers. It supports integration of other directory services, and supports multiple authentication protocols.

ADM provides IT professionals and administrative officers with both automated and manual ways to manage user and group accounts. With ADM, not only can you open, change, and delete accounts, but you can also create mailboxes in Exchange for an account, and add accounts to distribution lists.

ADM is also the background technology that will shortly provide all of NIH with automated account provisioning, updates, account transfer between ICs, and account deprovisioning—all of which are based on and synchronized to the changes to an individual's NIH Enterprise Directory (NED) account. ADM populates Active Directory resources such as shares and files and modifies permissions while enforcing policies and guidelines set forth by NIH. It can automatically add or remove members from groups, and can even be set to schedule the management of temporary group members.

Benefits

Controlled, secure administration: Because ADM acts as a security layer around AD, it helps administrators maintain compliance with security policies by enabling them to define administrative roles, set associated permissions, and enforce role-based rules. ADM ensures that AD management is secure and delegation of roles is reliable and controlled.

Effective auditing and reporting: ADM provides an audit trail that details who performed what actions on which accounts and when.

Web availability: ADM offers administrators, self-service users, Help Desk, and data owners a dynamically configured and customized web interface that follows all the same rules that are in place via the console.

More information

For more information regarding ADM, contact the NIH Help Desk at http://ithelpdesk.nih.gov/support, or by phone at 301-496-4357 (6-HELP) (local), 866-319-4357 (toll free), or 301-496-8294 (TTY).

Live Upgrade Now Available on Hosted Sun Solaris Servers

CIT has recently started implementing Live Upgrade on hosted Sun Solaris servers provided through our Unix Hosting Services. This allows system administrators to apply operating systems patches or perform an operating system upgrade with minimal downtime and disruption to the system.

How it works

To enable the live upgrade feature, the system is set up with a duplicate operating environment. Before patching, the active environment is duplicated, and the patching or upgrade is performed on the inactive copy of the operating system environment. Using this method, the updates can be done at any time without affecting running applications, which means they have no impact on normal system operations.

A system reboot is all that is needed to have the new environment become active; when the system is rebooted, the updated/patched version becomes the current boot environment.

Live Upgrade benefits

Shortened outage time: Patching with Live Upgrade lowers the system's downtime considerably. A patch or upgrade done without Live Upgrade could involve an outage of two to six hours. When patching with Live Upgrade, on the other hand, the outage is usually limited to a single reboot—10 to 20 minutes depending on the type of hardware.

For example, in the past four weeks it was necessary to have a few patching outages on hosted servers. The ones done without Live Upgrade required 191 and 201 minutes of downtime respectively, while the ones using Live Upgrade lasted less than 15 minutes (14 and 12 minutes, specifically), thereby reducing server downtime by at least 177 minutes, or almost 3 hours.

Minimal application outages and easy restore of prior versions: Live Upgrade's use of a duplicate operating environment also ensures that, if problems do occur with a patch or upgrade, the previous version of the OS is still available. Thus, the fallback to the previous version can easily be completed by rebooting back to that environment.

Unix Hosting Services

CIT's Unix Hosting Services offer centrally supported, dedicated, shared, and virtual Unix servers in a fully managed, 24x7 hosted environment. Our services include managed storage and backup, SSL certificates, network security architectures, application firewalls, load balancers, central web and database services in shared and dedicated configurations, and disaster recovery offerings. We provide a secure, SAS 70 audited environment with high availability configurations which includes patching, monitoring, and a dedicated customer coordinator.

More information

For more information about running your applications on CIT's hosted Sun Solaris servers or if you have questions about Live Upgrade, contact the NIH Help Desk at http://ithelpdesk.nih.gov/support, or by phone at 301-496-4357 (6-HELP) (local), 866-319-4357 (toll free), or 301-496-8294 (TTY).

Titan Default Printer Switches to Cut Sheet

As part of greening the NIH Data Center, Titan's default centralized printing will change from continuous-form paper to cut-sheet paper starting on November 15, 2009. Facing rising energy costs and concerns about sustainability, data centers worldwide are looking for ways to reduce the consumption of power and natural resources. At 30-40 percent of the operational budget today, energy usage is becoming the NIH Data Center's largest single operating cost. As reported in the Spring 2009 *Interface* article "Going Green by Increasing Printing Efficiency"(issue 243), the maintenance costs for the 3900 continuous-form printers have been increasing steadily, due to the energy use and need for special equipment associated with these printers.

We encourage you to consider alternate—and often lower-cost—ways of viewing your Titan output. The Data Center is ready to assist you in identifying the option that best fits your needs. Together we can find alternatives to continuous-form printing that help both the environment and the bottom line.

Do I have to change my JCL to use cut-sheet printers to generate the output?

Starting on November 15, 2009, the default printer for centralized output generation will be the cut-sheet printer. No JCL (Job Control Language) changes will be required to generate the output on cut-sheet printers as of the November 15th date.

The default print service will feature double-sided, cut-sheet forms in landscape mode. Available options include portrait mode, single-sided printing, and 3-hole-punched paper. In addition, there are slower impact printing services for labels and user-supplied forms.

Alternatives to continuous-form printing

There are a number of alternatives to continuous-form printing you can select that are cheaper and greener:

1. Use IOF (Input Output Facility) in *TSO/ISPF* to save output on disk.
2. Use IOF as a *batch job* to save jobs/reports to a Titan data set.
3. Use JCL to route reports directly to a Titan data set.
4. Use JCL to fetch job output and email to recipients.
5. Use JCL to fetch job output and convert it to a PDF file and email it to user.
6. Use a cut-sheet printer to generate the output.

Benefits of alternatives to printing output:

- Save on printer costs – it can be cheaper to save reports on disk or as PDF files.
- Gain office space that is now used to store printed output.
- Reduce the time spent searching for specific data – it's easier to find in media-stored output.
- Print only what you need and help NIH achieve its Greening Goals.

Making the switch

The remainder of this article describes how to use each of these greener (and cheaper!) alternatives.

1 - Use IOF in *TSO/ISPF* to save output on disk—The *Interface* article "Going Green by Increasing Printing Efficiency" (http://datacenter.cit.nih.gov/interface/interface243/output.html) describes this technique. To save on your printing costs and reduce the physical space needed for storing and filing printouts, consider using the ISPF Input Output Facility (IOF) to save your job output as disk data sets instead of printing it. You can always print the job from the data set at a later date or edit the data set and then print the output. To avoid printing, you must hold the output using either MSGCLASS=H with SYSOUT=* or /*ROUTE OUTPUT HOLD.

2 - Use IOF as a Batch Job to save output on disk—Instead of using TSO/ISPF, a batch job that executes IOF can be used to save output on disk. Let's assume a userid, JOEUSER, has several jobs in output hold that could be saved to disk:

The example below lists all jobs in the output queue belonging to userid JOEUSER.

```
------------------------------ IOF Job List Menu -------------( 4 )------------
COMMAND ===>                                                 SCROLL ===> DATA
--------------------------------- Output Jobs ---------------------------------
-------JOBNAME--JOBID---ACT-STAT-OWNER----DEST/DEVICE-------RECS-HELD-DAY--TIME
_    1 JOB1     J002621        8 JOEUSER  NIHJES2                1664 037  5:01
_    2 JOB2     J002112          JOEUSER  NIHJES2                5342 037   :13
_    3 JOB3     J001918          JOEUSER  NIHJES2                1787 036  5:01
_    4 JOB4     J001440          JOEUSER  NIHJES2                5342 036   :17
```

On August 22, 2009, JOEUSER wishes to run the IOF batch utility, BATCHTSO, to save JOB4 (job number = J001440) to disk as a dataset named JOEUSER.JOB4.AUG2209. The following JCL would save the job to disk as data set JOEUSER.JOB4.AUG2209:

- //SAVE2DSK EXEC BATCHTSO
- //OUTPUT DD DSN=JOEUSER.**JOB4.AUG2209**,DISP=(NEW,CATLG),UNIT=FILE,
- // DCB=(LRECL=133,BLKSIZE=0,RECFM=FBA),
- // SPACE=(TRK,(10,10),RLSE)
- //SYSTSIN DD *
- %FETCH **J001440**

3 - Use JCL to route reports directly to a Titan data set

- //STEPNAME EXEC PGM=*your program*
- //*outputddname* DD DSN=USERID.REPORT.NAME,DISP=(NEW,CATLG),
- // UNIT=FILE,DCB=(LRECL=133,BLKSIZE=0,RECFM=FBA),
- // SPACE=(TRK,(10,10),RLSE)
- //*OTHERDD*

4 - Use JCL to fetch job output and email to recipients

- //STEP1 EXEC BATCHTSO
- //OUTPUT DD DSN=*USERID.Report.Name*,DISP=(NEW,CATLG),
- // UNIT=FILE,DCB=(LRECL=133,BLKSIZE=0,RECFM=FBA),
- // SPACE=(TRK,(10,10),RLSE)
- //SYSTSIN DD *
- %FETCH *J031951*
- /*
- //STEP2 EXEC SENDMAIL
- //SMTPOUT DD SYSOUT=(M,SMTP),FREE=CLOSE
- //MAILIN DD *
- FROM: *SENDEREMAILADDRESS*
- TO: *RECEIVEREMAILADDRESS*
- SUBJECT: *Your Report Subject*
- *Text from your email body*
- //ATTCNTL DD *
- ASCII01; APPLICATION; *Your report2.txt*
- //ASCII01 DD *DSN*=USERID.*Report.Name,DISP=SHR*

5 - Use JCL to fetch job output and convert it to a PDF file and email it to users

- //STEP1 EXEC BATCHTSO
- //OUTPUT DD DSN=*USERID.Report.Name,*DISP=(NEW,CATLG),
- // UNIT=FILE,DCB=(LRECL=133,BLKSIZE=0,RECFM=FBA),
- // SPACE=(TRK,(10,10),RLSE)
- //SYSTSIN DD *
- %FETCH *jobnumber*
- /*
- //PDF EXEC PGM=IKJEFT01,DYNAMNBR=100,REGION=0M
- //SYSEXEC DD DSN=NIH.CLISTS.VB,DISP=SHR
- //SYSTSPRT DD SYSOUT=A
- //SYSTSIN DD *
- %TXT2PDF 'ORIENT=LANDSCAPE,CC=YES,TITLE=YOUR REPORT'
- //SYSUT1 DD DSN=*userid.report.name,*DISP=SHR
- //SYSUT2 DD DSN=*userid.report,name.PDF,*DISP=(NEW,CATLG),
- // UNIT=FILE,RECFM=VB,LRECL=256,DSORG=PS,
- // SPACE=(TRK,(5,5),RLSE)
- //EMAIL EXEC SENDMAIL
- //SMTPOUT DD SYSOUT=(M,SMTP),FREE=CLOSE
- //MAILIN DD *
- FROM: Senderemailaddress
- TO: Receiveremailaddress

- SUBJECT: *Your Report Subject*
- *Text from your email body*
- //ATTCNTL DD *
- BINARY01; APPLICATION/PDF; yourreportname.PDF(attachment name on your email)
- //BINARY01 DD DSN=userid.report.name.PDF, (from Step 2)
- // DISP=SHR

Conclusion

Reducing Titan's dependence on the 3900 continuous-form printer will help us lower one of our largest single operating costs—energy usage—and bring the NIH Data Center in line with NIH greening goals (http://www.nems.nih.gov) of sustainability and reduced resource consumption. We hope to work with our customers to achieve our goals of becoming more energy efficient and increasing our IT capacity without expanding our energy footprint from what it is today.

If you need help or have any questions regarding Output Distribution, contact the NIH Help Desk at http://ithelpdesk.nih.gov/support or call 301-496-HELP (301-496-4357), 866-319-4357 (toll free), or 301-496-8294 (TTY).

CIT Now Offers Windows and Unix Hosting Services at Off-Campus Site

In addition to our existing on-campus Windows and Unix Hosting Services, CIT is now offering the same full-service hosting at our off-campus Data Center site in Sterling, VA.

Off-campus hosting services

At Sterling, the Windows and Unix Hosting Services extend the secure, SAS 70-audited, fully-managed, 24x7-hosted environments already offered through our on-campus hosting service to our off-campus facility. Off-campus customers are supplied with centrally supported dedicated Windows and Unix servers, as well as services such as managed storage and backups, application firewalls, load balancers, and database services. CIT's full-service hosting at both locations includes patching, 24x7 monitoring,

technical support, dedicated customer coordinators, and collaboration on deploying secure and highly available application environments. Off-campus hosting still ensures the full confidentiality, availability, and integrity of NIH information.

The off-campus site

CIT's off-campus site in Northern Virginia (Sterling)—approximately 30 miles away from the NIH campus—is a secure commercial location run under the auspices of CIT and connected to NIH by an extremely high bandwidth network. CIT is continuing improvements to the site and recently upgraded the network connectivity to accommodate the growing volume of customer data.

Because of its location, off-campus hosting offers additional options to customers interested in high availability and disaster recovery configurations for their hosted servers so that business can continue uninterrupted in the event of an application outage or disaster.

More information

For more information on the services offered, please consult the CIT Service Catalog or contact the NIH Help Desk at http://ithelpdesk.nih.gov/support, or by phone at 301-496-4357 (6-HELP) (local), 866-319-4357 (toll free), or 301-496-8294 (TTY) if you have any questions.

The End of Wylbur

As announced in previous issues of *Interface* and *Titan News*, Wylbur, the Titan mainframe editing and batch processing system, will retire on **December 31, 2009**.

Resources

CIT is offering a number of resources to help Wylbur users find alternatives to their Wylbur procedures and processes.

- The Wylbur Retirement website at http://silk.nih.gov/silk/wylbur is a central source of information about the transition and the different types of assistance available for Wylbur users.

- The Wylretire Wiki (http://wylretire.cit.nih.gov) offers a growing library of information on the various alternate tools for Wylbur procedures, including advice on using ISPF for basic mainframe tasks.
- *Titan News* (http://datacenter.cit.nih.gov/titannews/) has been featuring a series of articles on Wylbur alternatives.
- The CIT Computer Training Program offers classes on ISPF, a full-screen editor in TSO. Check the Training website (http://training.cit.nih.gov/) for course offerings such as "Introduction to ISPF."
- In some cases, CIT can arrange for small group consulting for an office or group of people who support an application using Wylbur. Please see the related article "Small Group Consulting on Wylbur Retirement Issues" in issue 244 of *Interface* for more details.

We want to hear your questions and concerns

We want to hear from you and make sure we address your concerns. Please contact the NIH Help Desk at http://ithelpdesk.nih.gov/support or 301-496-4357, 301-496-8294 (TTY), or toll free at 866-319-4357 with your questions and requests for assistance. To keep up with the latest news on the Wylbur retirement, subscribe to the *Titan News* online newsletter.

CIT Computer Training Program Update

Updated website

This fall, as you may have noticed, the website for the CIT Computer Training Program has been completely redesigned to have a sleek new look and functionality. Users can now access a complete listing of all courses, register online for an upcoming session, view transcripts, and even see how many seats are still available in a session by visiting http://training.cit.nih.gov. We also encourage you to subscribe to the CIT Training listerv (distributed monthly) and/or RSS (Really Simple Syndication) feeds that will alert you as additions to the course schedule are made (for more on RSS, see "RSS at NIH" in *Interface* #239).

A revolving term

CIT Computer Training has also implemented a revolving term that will correspond with the fiscal year so you won't have to wait for a new term to start before registering for courses.

Courses on Section 508 compliance

Most of our courses are free of charge to NIH staff and as the training program evolves, we are able to offer new training opportunities. As many know, Section 508 was enacted to eliminate barriers in information technology, make available new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals. To help with this initiative, we are offering sessions in creating compliant PowerPoint presentations and Word documents. Stay tuned for sessions in the screen-reading software program JAWS (Job Access With Speech).

Available courses

New courses being offered through our program are:

- Pathogen Analysis using BEAST
- Molecular Graphics: Illustrations with PyMOL, Chimera, and VMD (I and II)
- Biomedical Illustration and Animation with Blender
- GIMP: Free Alternative to Adobe Photoshop

Popular courses returning:

- MATLAB for Scientists
- Better Graphics with R
- Statistical Analysis of Microarray Data
- Excel 2007 Formulas and PivotTables
- Office 2007 – What's New?
- QVR – Introduction, Intermediate, and Advanced
- ECB – Council Information Management, Advanced Project Data Administration, and Early Concurrence Data Administration
- Wiki Tutorial
- Adobe Photoshop Hands On

Questions?

If you have any questions about the CIT Computer Training program you may give us a call at 301-594-6248 or send an email to CITTraining@mail.nih.gov.

Directories and Reference Information

NIH Computer Center Hardware and Software

[http://cit.nih.gov/ProductsAndServices/ApplicationHosting/RelatedServices/HardwareSoftware.htm]

Computer Services Telephone Directory

[http://cit.nih.gov/NR/rdonlyres/CD8200B2-35E6-424C-A1C9-48DA35CE8155/0/TelephoneDirectory.pdf]

Online Services Directory

[http://cit.nih.gov/ProductsAndServices/ApplicationHosting/AboutDataCenter/OnlineServices.htm]

Popular Websites for NIH Computer Center Users

[http://cit.nih.gov/ProductsAndServices/ApplicationHosting/AboutDataCenter/PopularWebSites.htm]

Major Contributors

Laura Bennett, DCSS
John Dussault, DCSS
Sarah Fichter, DCSS
Robert Klein, DCSS
Katherine Matthews, DCSS
Michael Melinchok, DECA
Paula Moore, DCSS
Michele Schwartzman, DCS
Norma Stern, DCSS
Chantel Walker, DCSS

DCS	Division of Customer Support
DCSS	Division of Computer System Services
DECA	Division of Enterprise and Custom Applications