Procedures for Deregistration Officials and Account Sponsors

April 2008

National Institutes of Health
Center for Information Technology
NIH Data Center
12 South Drive MSC 5607
Bethesda, Maryland 20892-5607

Publication No. CIT150A

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The institutes and centers (ICs) of the National Institutes of Health (NIH) maintain sensitive financial systems that require strong security procedures and sound management practices. Among the important financial and management controls is the deregistration of unauthorized users, such as those NIH employees and contractors who leave the NIH or transfer between ICs. Deregistration denies the unauthorized user access to the computing services provided by the Center for Information for Technology (CIT) — specifically from the z/OS (mainframe) Titan System and its operating environment, which includes the Administrative Data Base System (ADB). Denying access to employees and contractors who have left the IC is a good management practice: it prevents unauthorized access to IC data, and the resulting potential resource cleanup can save IC funds by avoiding unnecessary computer charges.

This manual provides the registration and deregistration guidelines required for deregistration officials and account sponsors. Account sponsors must ensure that their CIT registered users — authorized to specific accounts — have the correct authority to expend IC monies. The manual also provides an introduction to RACF security requirements and Web Sponsor, the online account management tool.

The deregistration process contains two phases. The first is to deny access of unauthorized personnel from financial applications and the systems they run on. The second involves the cleanup of resources the person utilized (which is the responsibility of the account sponsor, not the deregistration official). Web Sponsor, described in Section 4, helps account officials carry out these tasks.

We recommend that this manual be used as a training guide for new staff between formal training offerings, or in place of training offerings when resources are scarce.

1.1. Assistance

If you need assistance with accounts or other CIT services, contact the NIH Help Desk.

Phone: 301-496-4357 (6-HELP) (local)
866-319-4357 (toll free)
301-496-8294 (TTY)
Web: **http://ithelpdesk.nih.gov**

For other forms of assistance, see Section 8.

1.2. Note for Non-NIH Users:

The terms “Executive Officer” or “EO” may be thought of as a “Program Official” or “Security Officer” for non-NIH agencies. Similarly, the term “IC” (for institute or center) may be thought of as a non-NIH agency (e.g., Nuclear Regulatory Commission).

Unless otherwise stated, the procedures described in this publication are the same for both NIH users and non-NIH users.

2. ORIENTATION

2.1. Center for Information Technology (CIT)

CIT provides, coordinates, and manages information technology and works to advance computational science. To accomplish this mission, it provides a variety of data processing services on a cost-recovery basis to the NIH and other government agencies. CIT supports the NIH’s research and management programs with efficient, cost-effective information systems, networking services, and telecommunications services.

CIT manages the multi-platform NIH Data Center for application and Web hosting, including co-location and disaster recovery services; and the Helix systems for NIH scientists.

For more information about CIT, visit the CIT home page [**http://cit.nih.gov**].

2.2. CIT Account Numbers

Anyone who wishes to use the NIH Data Center services must first obtain a CIT account. The appropriate account authorization forms are available from the CIT Accounts Web page [**http://support.cit.nih.gov/accounts**]. Select the link “Forms” at the bottom of the page. Please note that there are separate forms for NIH and non-NIH customers. The account identifies the customer or organizational unit responsible for reimbursing CIT for the charges that will be incurred. An account may have one or many authorized users. Persons who are already registered users can request account authorization forms via Web Sponsor (see Section 4).

2.3. Userids

In addition to the account number, each customer will be issued a userid (once known as an “account/initials combination”). Userids are the identifiers for individual users and have the following characteristics:

- Userids may be from 2 to 8 characters long, with the first character an alphabetic letter or a $. TSOids are limited to 7 characters in length. Userids of 8 characters cannot log on to TSO.
- In order to avoid problems, users who expect to develop applications that use UNIX System Services should not have userids that include a $. In particular, data set names incorporating a $ are treated differently under UNIX Systems Services.
- Each userid is associated with one, and only one, account.
- The userid, TSOid, and RACFid are identical.
- User-owned data sets must begin with either the userid—with the form *userid*.name (e.g., johndoe.dataname)—or with the account (e.g., aaaa.dataname or aaa.dataname).

2.4. Output Box Numbers

Userids must be associated with an output box number. The default output box for new customers is NOBX. If customers do not need a secure box for printed output, they can use “NONE” as a valid output box number. To view or change the output box number, use Titan Customer Locator [**http://titan.nih.gov/locator**]. Refer to the *Titan User's Guide* for more information about output boxes.

2.5. Proper Use of Computing Facilities

Users and account sponsors are responsible for the proper professional use of their accounts and userids and the government facilities accessed through them. Users should be individually registered and should not allow their userids to be used by anyone else. Use of computer time for such things as games, personal records, outside business activities, etc. is illegal. For further information see the *Titan User's Guide*, which can be viewed online, printed, or ordered or by visiting the CIT publications Web page [**http://publications.cit.nih.gov**]. Select the topic “NIH Data Center User’s Guides.”

Users should also refer to the NIH Information Technology General Rules of Behavior [**http://irm.cit.nih.gov/security/nihitrob.html**].

3. SECURITY AND RACF

The HHS Information Resource Management (IRM) policy requires data centers to provide access-control software to users for protection against unauthorized access to computer facilities. The NIH Data Center supports RACF for access and data security for the mainframe system and to allow users to maintain additional data protection. All userids are automatically registered to RACF for access and data protection.

Each CIT account must have a security coordinator who serves as the point of contact for CIT security matters. For more information, see Section 7.2.

Consult the *Titan User's Guide* for more information on userids and details about RACF and NIH Data Center security.

3.1. RACF (Titan) Passwords

Resource Access Control Facility (RACF) passwords are used to gain access to Titan (e.g., TSO, ISPF, NIH WYLBUR, DB2). All users are automatically registered to RACF when they obtain their userid. Users need only specify the RACF password that is in effect for their userid, to gain access to Titan. The password has the following characteristics:

- It must be 7 or 8 characters.
- The password must include at least one alphabetic character, at least one numeric character, and at least one special character.
  - The special characters used in the password are limited to these: #, @, or $.
- It cannot be the same as the Titan userid.
- RACF passwords expire every 60 days.
- When a RACF password expires, you may not reset it to any of your 24 previous passwords.
- It cannot be changed more than once a day.
- If users know their existing Titan password, they can change their password via the Web RACF interface [**http://titan.nih.gov/racf**]. If users do not know their existing Titan password, see Section 3.1.2 for information on resetting forgotten passwords.

NOTE: Titan does not distinguish between upper and lower case, therefore changing the case of an alphabetic character does not change the password.

Although the requirements for a RACF password and the NIH Login password are very similar, CIT strongly recommends that you do not make both passwords the same. This minimizes the chance that a compromised NIH Login password could be used to access Titan.

3.1.1. Forgotten Passwords

Users who forget their passwords or who mistype a password repeatedly will not be able to log on. Users should never try to guess a password that they have forgotten. Typing errors could generate a security message such as INCORRECT RACF PASSWORD (RECORDED IN SECURITY LOG). While typing errors are expected, users should not attempt to enter the RACF password more than three or four times. After that, the account sponsor should be contacted. Repeated password entry errors are logged in Data Center security logs, and can trigger a security violation. CIT then revokes the use of the userid until a security investigation is completed.

Due to the design of RACF, it is impossible to determine the password for a userid; instead the password must be reset. The user can ask the account sponsor to provide a temporary password. The password the account sponsor provides is automatically expired. See Section 3.1.2 for specific information on resetting forgotten passwords.

For more information on security violation procedures at CIT, refer to the *Titan User's Guide*.

3.1.2. Resetting Forgotten Passwords

Information on resetting forgotten passwords is available online [**http://silk.nih.gov/silk/sponsorinfo**].

Here are some options:

- **Password Reset** - Users associated with NIH, who have an NIH Login, can reset their own Titan passwords using the Password Reset Web page [**http://silk.nih.gov/passwordset**], provided their NIH ID badge number is associated with their Titan userid. Users can Log in to the Password Reset page with their NIH domain credentials. Once users successfully log on, they will see the “Titan Password Reset” interface where they can set a new Titan password. Password Reset can also be used to reset Helix passwords.

  Note: If you are associated with NIH and you forget your NIH Login password, contact the NIH Help Desk. As an alternative to calling the NIH Help Desk, you can register for the CIT self-service password management tool, iForgotMyPW, which allows you to reset your NIH password or unlock your account yourself. You must pre-register for this service [**http://iForgotMyPW.nih.gov**] and follow the instructions. If you know your NIH password and would like to change it, go to: **https://password.nih.gov/**.

- **Web Sponsor** - An account sponsor can use Web Sponsor [**http://websponsor.cit.nih.gov**] to reset a user’s forgotten RACF password. (See Section 4.2 for other ways to access Web Sponsor.) Passwords reset by the account sponsor via the Web Sponsor interface automatically set to an expired password. The user must then change this password before they can successfully log on to the system by going to the SILK Web page [**http://silk.nih.gov**] and do the following:

  - At the SILK Web page, select the link “Security (RACF).”
  - Log in with your userid and the temporary password provided by the account sponsor.
  - At the screen with the message “Your MVS Password Has Expired,” select the link “Change Password Now.”
  - Next, change the temporary password to a new one.

- **Fax a request** - As a last resort, fax a request to CIT security investigators at (301) 496-6905 to reset a forgotten password. They can reset the password within 24 business hours.

3.2. Do You Have a Safe Computing Environment?

Protect your account; change your RACF passwords frequently. The NIH CIT recommends changing passwords at least once a month. Avoid using passwords that can be guessed easily. Even though NIH Data Center output does not divulge any password information, security can be compromised over time in subtle ways (e.g., workstations that cannot mask passwords that are entered when signing on to an application or by users who post passwords on “post-its” near workstations).

Be particularly cautious about revealing your RACF password to someone on the telephone. If you feel your password has been compromised and others have signed on to Titan with your userid, call NIH Help Desk at 301-496-4357.

For additional information on IT security for NIH systems, visit the CIT Security Web site [**http://cit.nih.gov/security.html**].

3.3. Security Investigators

Security investigators are CIT staff specifically assigned to investigate apparent security violations. If CIT observes or perceives possible security violations, the CIT security investigators will contact the account sponsors of the account that is suspected.

The CIT security investigators offer consulting to help users address and/or avoid security problems in the use of CIT-provided services. Please call the NIH Help Desk and ask to consult with a security investigator.

4. USING WEB SPONSOR FOR ACCOUNT MANAGEMENT

4.1. What is Web Sponsor?

Web Sponsor is an automated account management tool written by, and supported by, CIT. Web Sponsor facilitates account management procedures for the account sponsors, as well as deregistration officials. Web Sponsor supplies deregistration officials and account sponsors with all the necessary information needed to properly administer their accounts.

Web Sponsor allows deregistration officials and account sponsors to display information about a specific account, all accounts, or all accounts under a specific common account number (CAN). Sponsors and deregistration officials can also reset RACF passwords online, averting the faxing of requests to the security investigators. Passwords that are changed via Web Sponsor are automatically set to expire.

Billing coordinators and security coordinators for an account (see Section 7) can also access some functions of Web Sponsor. However, Web Sponsor will only let account officials do what they are allowed to do based on their role—sponsor, deregistration official, billing coordinator, or security coordinator.

4.2. Accessing Web Sponsor

There are several ways to access Web Sponsor.

- **Go to: http://websponsor.cit.nih.gov**

  The first time the Web Sponsor page is accessed from a Web browser, a security "pop-up" window prompts for a userid and RACF password. Only account sponsors with valid userids and passwords will be allowed to display and change data for their account.

- **Web Sponsor through the NIH Login**

  If you are associated with NIH, you also have the option of accessing Web Sponsor through your NIH Login via the Web [**http://websponsor.cit.nih.gov/nihlogin**].

- **Web Sponsor via the NIH Portal**

  NIH Portal users who have personalized a my.NIH.gov Web page can access Web Sponsor through its own portal "portlet." If you are an account official and have a NIH Login, go to: **http://my.nih.gov**.

  Log in with your NIH user name and password. Click on the online help at the top of the page and follow the instructions for adding portlets. You can place the Web Sponsor Launch Pad portlet on your own my.NIH.gov page [**http://my.nih.gov**].

4.3. Web Sponsor for Deregistration Officials

- **Display information for decision making**

  Web Sponsor provides several ways to display user information to deregistration officials:

  - Web Sponsor displays all accounts for which the deregistration official is responsible, as well as the names of sponsors associated with those accounts. These accounts and the associated information can be sorted by the IC name along with the common account number (CAN). This is under Accounts>>Display - Account Official Information.
  - For a specific userid (userid, NIH ID, or Helix ID), deregistration officials can view information about the account (and the names of the account officials). This is under Customers>>Display - Customer information
  - For a user's name, the deregistration official can see all of the accounts to which the user is registered (with IC, CAN, and sponsors). This is under Customers>>Display - Customer information
  - For a specific account or all the accounts, the deregistration official can view account official information, all userids registered (complete with address and phone number). This is under Accounts>>Display - Customer Information.

- **Resetting RACF (Titan) passwords to deny access**

  Resetting RACF passwords through Web Sponsor causes immediate denial to the Titan system. Departing employees or contractors will no longer be able to access systems and data once the password is changed. It is wise to use Web Sponsor and reset the password on the employee's last day. CIT strongly encourages that RACF passwords be immediately reset for departing, disgruntled employees or contractors. If this is not done, data may be maliciously altered or destroyed. Password changes are recorded in an auditable log.

  - To reset (change) a password for a user, go to Customers>>Security-Change Titan Password.

Deregistration officials must not share their RACF passwords under any circumstances. The ability to reset passwords must not be shared. Inappropriate password resetting may cause loss or misuse of government resources and damage to critical program applications and/or data.

There is one, and only one, RACF password per userid. CIT does not have a strict policy as to whether a userid can be retained by an individual moving to another IC or agency. This is up to the parties involved. Special consideration is needed, however, before employees can take their userids to a new job where they will also use the NIH Data Center services.

- **Revoking userids**

  As an alternative to resetting the password for the userid of someone who leaves, sponsors can select Revoke Userid from the Web Sponsor menu (under Security). This means that the userid will no longer be able to log in to the system or run batch jobs. Sponsors may restore access privileges for a userid (Restore Userid) as soon as they are confident that no breach of security was attempted.

5. DEREGISTRATION OFFICIALS

5.1. Appointment of Deregistration Officials

Deregistration officials for the NIH are appointed by the IC executive officers. For non-NIH federal agencies, the appointments are made by an agency official responsible for account maintenance, by a program manager, or by a security official. These executive officers and agency officials are also responsible for ensuring that the deregistration officials chosen are qualified people. Since responsibility for information accuracy involves issues of expenditure of funds, security, and privacy, the deregistration official **must always be a government employee**.

Only one primary and alternate deregistration official are permitted for each account, and each must be a registered user of the NIH Data Center. When a deregistration official leaves, for whatever reason, the executive officers are responsible for quickly appointing a replacement.

Executive officers and program officials can designate/authorize a deregistration official and an alternate deregistration official by completing the Deregistration Official Authorization form, and forwarding it to the NIH Help Desk. To obtain a copy of the form, go to the CIT Accounts Web page [**http://support.cit.nih.gov/accounts**] and click on Forms at the bottom of the page.

Alternate Deregistration Officials
The deregistration official must have a backup—a formally assigned alternate who has the same employment profile described above. The alternate deregistration official must be designated using the Deregistration Official Authorization form (signed by the IC executive officer or the agency program officials).

For further assistance on appointing a deregistration official, please call NIH Help Desk and ask to speak to someone in Customer Accounts. See Section 1.1 for the phone numbers.

5.2. Responsibilities of Deregistration Officials

The ultimate responsibility, within the IC or federal agency, for the accuracy of computer access information belongs to the deregistration official.

The major responsibilities are as follows:

- When new accounts are opened, CIT requires that the paperwork be initialed by the account's deregistration official, indicating receipt. The deregistration official does *not* approve the account opening, nor is it an authorizing signature. This ensures that each account opened is assigned a deregistration official.

- Deregistration officials should be authorized to use Web Sponsor [**http://websponsor.cit.nih.gov**], the Data Center’s account management tool. For information on Web Sponsor, see Section 4 of this manual or the *Titan User's Guid*e.
- The primary and most crucial responsibility of the deregistration official is to ensure that the employee’s RACF password has been reset, or the userid deleted, after the employee has left the IC or agency. This will ensure that sensitive data can not be tampered with after the employee’s departure, and satisfies the Office of Inspector General’s financial audits.
- The primary deregistration official can add/change/remove account sponsors, including selecting a new primary account sponsor.
- It is the deregistration official’s responsibility to ensure that the account sponsors (primary and alternate) select one of their Titan userids to be the sponsor userid. This can be done through Web Sponsor.
- Deregistration officials who have more than one Titan userid are encouraged to select one Titan userid to be used to perform deregistration official duties. This userid will be recognized by software at the NIH Data Center and will provide the proper authorities for all deregistration actions.

CIT's technical newsletter, *Interface* [**http://datacenter.cit.nih.gov/interface**] and the online publication *Titan News* [**http://datacenter.cit.nih.gov/titannews**] will announce any changes at the NIH Data Center that might affect the role of deregistration officials. You can subscribe to these Listserv lists directly from their Web pages.

5.3. Working with Account Sponsors

Deregistration officials work with account sponsors on the deregistration process. The deregistration official can be the same person as the account sponsor. There are account sponsors for all CIT accounts — a primary and one or more alternates. The account sponsor is the IC official responsible for the maintenance of the resources that the IC employees and contractors are paying for and using at CIT for a specific account. These responsibilities have been in place for over 30 years, and are documented in the *Titan User's Guide* and in this document. See Section 6 for information on account sponsors.

Account sponsors have the primary responsibility for removing departed/inappropriate users from their account. “Clean-up work,” (e.g., getting rid of data sets, removing databases, releasing tapes, etc.) is done solely by the sponsors (see Section 6.5). It is the responsibility of the deregistration official to ensure that the proper deregistration of departed employees has been completed in a timely manner.

6. ACCOUNT SPONSORS

6.1. Importance of Account Sponsors

Account sponsors play a vital role in the success of the IC computer applications that run at the NIH Data Center. IC management can appoint sponsors at their discretion. Because of their importance, each sponsor should have at least one designated backup or alternate sponsor, for their accounts. The Center for Information Technology (CIT) has only one regulation on who can be an account sponsor; the person **must be a government employee**. Since sponsors can be responsible for budgetary and financial issues, the appointed person may not be a contractor.

When a new account is opened, the authorizing official designates the initial primary and alternate account sponsors on the CIT Account Request form.

CIT requests that IC managers designate account sponsors who have some understanding of NIH Data Center operations. Sponsors should be willing to adapt to technological changes and be readily accessible to the employees and coworkers who will be authorized to use the CIT account. They have full responsibility of their CIT accounts. The account sponsor can be the same person as the deregistration official.

Account sponsors are urged to take advantage of the wide variety of services described in the *Titan User's Guide,* and the extensive classroom training offered through the CIT Computer Training program. See Section 8 for further information.

CIT wants to be kept informed of problems encountered by account sponsors and would like to hear about your concerns. Communication, of course, must always be a two-way street. Occasionally, sponsors will be contacted in order to update information or if a problem arises concerning the user of an account. Be available. For this reason it is important for account sponsors and deregistration officials keep their directory information up-to-date through the NED [**http://ned.nih.gov**]. See Section 6.3 for more information.

The NIH Help Desk serves as the central point of contact for all CIT accounts and welcomes inquiries from sponsors concerning administrative procedures. If you have a concern about your account or account security, please contact them. See Section 1.1.

6.2. Responsibilities of Account Sponsors

- Registering an alternate sponsor (and specifying a Titan sponsor userid). This person will have the authority to act whenever the account sponsor is unavailable to ensure that the work of the organization will not be disrupted.
- Changing the NIH Common Account Number (CAN) to which the account is charged.
- Authorizing additional users on an account.

- Working with the IC deregistration official to ensure that all registered users are current employees or contractors of the responsible IC; have appropriate, approved access; and have current information on their user's records at CIT (e.g., name, address, phone number).
- Ensuring the appropriate use of federal computing resources by all users authorized on an account.
- Communicating with CIT on matters of security and privacy; reporting any suspected violation of password privacy to CIT's security personnel.
- Investigating possible security violations relating to a userid registered to the account sponsor's account.
- Reactivating a userid when security investigations are completed.
- Ensuring that all applications and data under their accounts are appropriately protected using the security facilities provided at the NIH Data Center.
- Ensuring that users are aware of their responsibilities for data security and access control.
- Determining when accounts are to be deactivated and ensuring that all chargeable items (e.g., tapes, publicly-stored data sets, etc.) and userids are deleted prior to deactivation.
- Working with the deregistration officials to deregister IC employees/contractors who leave NIH or transfer between ICs.
- Having the ultimate responsibility for user records and technical requirements needed for the "cleanup" phase of deregistration. Many of the tasks related to closing an account or removing a user from an account can be carried out through Web Sponsor. See Section 6.5.
- Resetting Titan passwords for users registered to your accounts.
- Reviewing the accounts and making any appropriate changes to the account information or to the names of the users authorized to use the account.
- Requesting remote access service (e.g., Parachute, VPN) and Helix accounts, when applicable, for users on your accounts. **Note**: remote access accounts have security policy requirements that are described in Web Sponsor.
- Assigning, reassigning, and removing alternate sponsors, billing coordinators and security coordinators
- **Primary sponsor only**
    - Designating a new primary sponsor

6.3. Web Sponsor for Account Sponsors

Use Web Sponsor (see Section 4.2 for access information) to change account sponsors, assign an alternate sponsor, display account log and information by account, change the CAN of an account, view bills, and close CIT accounts. There is online, comprehensive documentation included in Web Sponsor.

- **Resetting Titan passwords**

  Web Sponsor is the most effective tool for resetting Titan passwords. By using Web Sponsor, the account sponsor can reset the password. The password is automatically set to an expired password. Sponsors can also change the password expiration. As an alternative, the sponsor can send a fax to the CIT Security Investigators requesting to reset a password. However, fax requests can take up to 24 business hours before taking effect.

- **Display and change customer information**

  Use these options of Web Sponsor to fully display information about one of your accounts, all of your accounts, or accounts by CAN. Web Sponsor displays users registered to your accounts by userid, or by name, as well as showing addresses and phone numbers. Web Sponsor can also display DB2 objects associated with a user and a resource matrix (Web Sponsor displays the type of resources owned by the userid for the specified account as of 02:00 am the previous morning. These resources include data sets, tapes, Parachute/VPN authorization, Helix accounts, and Model 204 IDs).

  Web Sponsor and the NED
  Changes to directory information about users associated with NIH should be made by the users themselves through the NED (NIH Enterprise Directory) [**http://ned.nih.gov**]. Most information that is not updateable using self-service must be updated by an Administrative Officer (AO). Exceptions include the AD (Active Directory) domain and user name, which is updated by the NIH Help Desk, and in the case of government employees, home mailing address.

  Account sponsors can determine if users under their accounts have their NIH IDs in the Web Sponsor database by following these steps:

  - Access Web Sponsor.
  - Under Display click on the link to “Customer Information.”
  - Specify the type of ID and enter the user's ID
  - Click “Display.”
  - Click on the desired userid to open the record.

  The output will include the NIH ID, if it has been specified.

If the NIH ID has not already been specified, sponsors can use Web Sponsor to link the NED information to Web Sponsor.

Be aware that changes to the NED will carry over to Web Sponsor, but changes made directly through Web Sponsor will not be propagated to the NED.

Changing Information for Users Not in the NED
Account sponsors who work for other (non-NIH) government agencies can change Web Sponsor directory information for themselves and users under their accounts through Web Sponsor. Use the Change Customer Information facility.

- **Display account information**

  Web Sponsor displays account information, plus userid, name, and phone number of the sponsor, alternate sponsor, deregistration official, and alternate deregistration official for each account.

- **Validate, remove, reassign, and request new userids**

  One of the more important features of Web Sponsor — sponsors can add new users to their accounts, as well as remove users who have departed or no longer have authorization to use that account. Sponsors can reassign userids to new or existing users. New registered userids may be requested through Web Sponsor for new users to the account. Web Sponsor can also be used to request multiple userids for one particular user.

- **Perform Helix remote access/Model 204 registration and deregistration**

  Sponsors can register their users for Helix, remote access services (e.g., Parachute and VPN), and Model 204 via Web Sponsor.

- **Access CIT billing reports and the nVision Data Warehouse**

  CIT makes billing information available through Web Sponsor and the nVision Community of the NIH Portal. [**http://my.nih.gov**]

Web Sponsor - Account sponsors and billing coordinators can use the CIT Billing Reports link in Web Sponsor to view CIT charges for their account and for the individual users under their accounts. Use either:

http://websponsor.cit.nih.gov (requires your Titan userid and password)
or
http://websponsor.cit.nih.gov/nihlogin (requires your NIH Login User name and password)

nVision Community - Account sponsors, billing coordinators, and NIH nVision Data Warehouse Budget & Finance registered users can use the CIT Billing Reports facility. After entering the nVision Community, follow these steps to get to the

Billing Reports.

1. On the left side of the page, click on “Launch Reports.”
2. On the left side of the resulting page, click on the “plus signs” to open these folders in order:
    - Public Folders
    - Business Areas
    - Budget & Finance
3. Within the Budget & Finance folder, click on the Applications folder.
4. CIT Billing appears as one of the options within the Applications folder. Click on it to open up the CIT Billing Sign In screen.

The nVision Data Warehouse stores information that has been requested by the NIH business community. It is designed primarily to analyze business trends and performance. The nVision Data Warehouse acts as an information warehouse, providing integrated, historical business information from other NIH systems such as:

Administrative Database (ADB) - supports administrative and financial management activities.

Human Resource Information and Benefits System Database (HRIBS) - provides financial and personnel information on the NIH work force.

ITAS (Integrated Time and Attendance System) - a timekeeping by exception application that supports most aspects of tracking and reporting work hours and leave for federal employees. ITAS provides users with access to real-time leave balances and ensures that users accurately record work activity by enforcing time and attendance policies and procedures specific to the federal government.

NIH Business System (NBS) - The NIH Business System (NBS) is being built to replace the current Administrative Database System (ADB) and Central Accounting System (CAS). The NBS will provide administrative support to the scientific mission of the National Institutes of Health through cost-effective business solutions. The NBS Training and Communications Community is available through the NIH portal [**http://my.nih.gov**].

- **Account management**

  Sponsors can take actions that effect an account—such as closing the account, downloading a form to open a new account, changing the account title and CAN number, changing the primary sponsor, and adding or removing account officials.

- **Getting help with Web Sponsor**

  If you need assistance with Web Sponsor, refer to the included online documentation or call the NIH Help Desk at 301-496-4357 and identify yourself as a deregistration official or an account sponsor.

6.4. Important Deregistration Issues

- **Web Sponsor notification for users with an NIH ID**

  If users leave and their NIH IDs have been included in the Web Sponsor database, Web Sponsor sends e-mail to the account sponsors and deregistration officials for those accounts. Based on these e-mails, account officials can then determine when a userid must be removed or transferred to another user. (See Section 6.3 for information on linking NIH ID information with Web Sponsor.)

- **Work with departing staff**

  During the complete deregistration process, it is extremely important and critical that the account sponsor work with the departing employee or contractor and their supervisor. The employees or contractors should be very knowledgeable about the data sets and tapes they maintain — probably more knowledgeable than the account sponsor. Deleting data sets or releasing tapes with program-critical data could be fatal to the program mission. Be sure to consult with users who leave about the data they maintain. Critical data should be reassigned to another person involved in the program prior to termination.

- **Ramifications of reassigning userids**

  When userids are reassigned (i.e., the userids are given to another user), sponsors of the recipient of those userids should be aware of the resulting ramifications. Financial obligations are still incurred when the userids are reassigned. Any data sets, tapes, or other CIT-billable resources are still incurring charges to the account of the recipient. CIT strongly encourages the ICs to carefully review the situation — and see if the userids should be reassigned or just deleted.

- **Output box numbers**

  An output distribution box may have been assigned to the departing employee, or the employee may have been a courier for the IC. Each output box has an associated box access code (BAC), and most employees or couriers over a period of time, memorize the code. Depending on the nature of the employee’s departure, the employee could still try to gain access to the output box. Access to the output box could be of concern if the departing employee left on bad terms. If the deregistration officials or the account sponsors are concerned for the integrity of their data or tapes (items that may appear in the output box), they may call the NIH Help Desk and ask to speak to a consultant about box access codes.

6.5. Specific Requirements for Terminating Use of Services

Closing an account or removing a user from an account

Closing an account or removing a user from an account can only take place after meeting all of the requirements listed below:

- The account sponsor ensures that all computing resource usage has ceased.
- The userid no longer owns data sets or tapes.
- Data sets and tapes that contain important or useful data are transferred to another userid.
- All unneeded data sets are scratched and unneeded tapes released.

The steps required to reassign/release data and resources are listed below. Many of these steps can be accomplished through Web Sponsor, as indicated.

- **Reassign data sets by renaming them using another valid userid or account**. This places the data sets under the control of another user.
- An alternative is to **reassign the userid to an existing user** (Web Sponsor). When using these two methods (reassigning the data sets or reassigning the userids, the account sponsor should ensure that the resources are closely monitored.
    - Account sponsors should **reset the passwords** (Web Sponsor) for userids that will be reassigned and not deleted.
- Reassign ownership of tapes. Copy the entire tape and change the data set name of at least the first data set on the tape so that it begins with the userid of the new owner.
- Cancel subscriptions to Internet Listserv lists.
- Remove the userid when the cleanup is complete (Web Sponsor).

  A userid cannot be removed until all the resources associated with that userid are deleted. When a sponsor chooses this option, Web Sponsor helps the account sponsor perform functions such as:

    - deleting cataloged data sets
    - removing RACF profiles
    - scratching migrated data sets
    - deleting DB2 objects
    - removing the Web-based Job Scheduler entries

  After all the resources are removed, the account sponsor can delete the userid.

- If an account must be closed, first remove each userid in the account. Once the cleanup is complete, use Web Sponsor to close the account.

Contact the NIH Help Desk if there are any questions concerning the reassignment of userids or the deregistration procedure.

Immediately denying service for a userid

When it is necessary to immediately deny access to Titan for a userid (e.g., due to a suspected security violation), account sponsors should use Web Sponsor to reset the password or revoke the userid. If the userid has been revoked, the sponsor can restore the userid at a later time.

7. OTHER ACCOUNT OFFICIALS

There are two other types of account officials who help account sponsors fulfill their duties—billing coordinators and security coordinators. Account sponsors can take these roles themselves, or they can select other persons within the organization for these responsibilities. Sponsors assign and remove these officials using Web Sponsor.

7.1. Billing Coordinators

Each organization using the Titan system must have a billing coordinator, (usually a financial officer) assigned by the account sponsor. The billing coordinator deals with the financial aspects of an account. This official may be a contractor.

There must be one primary billing coordinator and any number of alternates. The billing coordinator receives invoices (primary billing coordinator only) for the appropriate accounts and can access billing data online through the nVision Data Warehouse or Web Sponsor.

7.2. Security Coordinators

Each user organization must have a security (RACF) coordinator. This function belongs to the account sponsor until the sponsor designates a security coordinator. The security coordinator may be a contractor. The security coordinator serves as the point of contact for CIT security matters and can change passwords for Titan (z/OS), Helix, and remote access users.

There must be one primary security coordinator and any number of alternates. Security coordinators carry out many of their functions through Web Sponsor and Web RACF. See the *Titan User's Guide* for more information on the role of the security coordinator.

8. CUSTOMER SUPPORT

8.1. General Assistance

Please contact: NIH Help Desk
Phone: 301-496-4357 (6-HELP) (local)
866-319-4357 (toll free)
301-496-8294 (TTY)
Web: **http://ithelpdesk.nih.gov**

8.2. Ongoing Training

Knowledge of current deregistration official and account sponsor responsibilities, along with CIT policies is crucial to each IC and other government agencies who use the NIH Data Center. The CIT offers training as part of the CIT Computer Training program for account sponsors and deregistration officials. Call the NIH Help Desk at 301-496-4357 to register for the next available seminar, or register online [**http://training.cit.nih.gov**].

8.3. Ordering Documentation

Ordering documentation from CIT is as easy as 1-2-double-click. Visit the CIT publication ordering facility on the Web [**http://publications.cit.nih.gov**]. This facility enables users to order, view, or print manuals and other types of documentation from CIT. If you need assistance with ordering publications, contact the NIH Help Desk.

Procedures for Deregistration Officials and Account Sponsors

Document Evaluation

Is the Manual:

	YES	NO
Clear?	□	□
Well organized?	□	□
Complete?	□	□
Accurate?	□	□
Suitable for the beginner?	□	□
Suitable for the advanced user?	□	□

Comments:

____

____

____

____

____

____

____

Please give page references where appropriate. If you wish a reply, include your name and mailing address.

Send to:
Applications Services Branch
Division of Computer System Services
National Institutes of Health
Building 12A, Room 4011
Bethesda, MD 20892-5607

FAX to: (301) 496-6905

ICD or Agency:
Date Submitted:
Name (Optional):
E-Mail Address:

4/08