Volume

1

NATIONAL INSTITUTES OF HEALTH

NIH Enterprise Directory

NED Overview

V13

NIH ENTERPRISE DIRECTORY

NED Overview

Center for Information Technology
National Institutes of Health
10401 Fernwood Road • Suite 300
Bethesda MD 20817

Revision History

Version	Date	Contributors	Summary
DRAFT 1	July 12, 2004	Keith Gorlen	First Draft
DRAFT 1		Keith Gorlen	Change title back to NED Overview
2	April 30, 2005	Keith Gorlen	Update for Remedy, BITS, and Oracle NED_PERSON_BASE.
3	December 27, 2007	Robert Malick	Updated NED physical diagram, hardware configurations, removed PH connector, renamed NHLBI eDirectory to Constellaiton Provisioning System, and updated some outdated concepts.
4	August 25, 2008	Robert Malick	Updated HHS Employee Directory info to indicate that this data now comes from NIH Active Directory. Remove nVision from Future Work section.
5	November 1, 2010	Robert Malick	Updated Figure 1 NED Physical System Diagram and Table 1 NED Connections Summary.
6	January 30, 2012	Robert Malick	Updated NED Physical System diagram and summary. Updated many sections.
7	May 29, 2012	Robert Malick	Removed references to HRDB, JEFIC and FPS2 systems.
8	November 13, 2012	Tom Bodine	Updated Figure 1 (NED Physical Diagram) to add back references to HRDB and FPS2, deleted JE connections to AD and ITAS (connections 16 and 28 respectively), and changed the connection 19 endpoint from LDAP Directory Server to Oracle.

Version	Date	Contributors	Summary
			Made corresponding updates to Table 1 (NED Connections Summary).
9	September 12, 2013	Tricia Fitzgerald	Removed references to JE decommissioning in June, 2012. Added reference to fsaAtlas decommissioning.
10	March 28, 2014	Tom Bodine	Updated the NED Physical System Diagram, Table 1 (NED Connections Summary), Table 2 (NED Production Server Configurations), Table 3 (NED Test Server Configurations)
11	April 23, 1014	Tom Bodine	Updated the NED Physical System Diagram Table 1 (NED Connections Summary) per Robert Malick comments.
12	March 18, 2015	Tom Bodine	Performed various updates to add additional content and remove out-of-date content. Added appendix A.
13	March 29, 2016	Tom Bodine	Performed various updates to remove out-of-date content.

Table of Contents

INTRODUCTION 7
Purpose 7
Benefits 7
NIH Environment 8
BACKGROUND 10
Information Technology Central Committee 10
Architectural Management Group 10
AMG Technical Subcommittee 11
NIH Identification Number 12
Privacy Act Clearance 13
Data Server Surveys 13
Directory Technology Assessment 14
Directory Steering Committee 14
NEDWeb Pilot Test and Deployment 15
NIH ID Badge and Card Access System 16
Meta-Directory Development and Deployment 16
NIH Login 17
Meta-Directory Upgrade 17
NED Corrective Action Plan (NED CAP) 18
Meta-Directory Decommissioning 18
FUNCTIONAL OVERVIEW 20
NED Workflow Application 20
NED Public Search 22
NED/AD Link Editor Application 22
PIV Sponsor Management Application 22
External Data Sources 23
Support for NIH Business Functions 23
On Boarding / Off Boarding 24
ID Badge Provisioning 24

NIH Network Account and Email Provisioning 25
Teleworking and Remote Access..... 25
NIH Parking and Transhare 25
NIH Library Services 25
NIH Telephone Directory and Operator Services 25
NIH Emergency Preparedness..... 25
NIH Staff Directory 26
NIH Annual Census..... 26
Data Broker..... 26
NED Physical System Diagram 28
Appendix A – NED Functional Interconnection Diagram..... 33

List of Tables

TABLE 1 NED Connections Summary 28
TABLE 2 NED Production Server Configurations 31
TABLE 3 NED Test Server Configurations 32

List of Figures

FIGURE 1 NED Physical System Diagram..... 28

Chapter 1

> We think we know what we are doing. We have always thought so. We never seem to acknowledge that we have been wrong in the past, and so might be wrong in the future. Instead, each generation writes off earlier errors as the result of bad thinking by less able minds—and then confidently embarks on fresh errors of its own.
>
> We are one of only three species on our planet that can claim to be self-aware, yet self-delusion may be a more significant characteristic of our kind.
>
> Michael Crichton, *Prey*

INTRODUCTION

Purpose

The NIH Enterprise Directory (NED) enables application programs and users to easily find information about the people who work at NIH. Mainly, NED contains information that **identifies** a particular individual, such as a person's name, unique HHS ID number, date of birth, place of birth, Social Security Number (SSN), and ID photo, and information to **locate** or contact a person at work or home, such as their email address, postal and delivery addresses, telephone numbers, organizational affiliation and status (Employee, Fellow, Contractor, Guest), and so on.

NED is the best source for NIH directory information because it includes all types of workers (Employees, Fellows, Contractors, Tenants, Guests, and Volunteers), it represents data values consistently to simplify searching and report generation, it is connected to NIH business processes for registration/deregistration, and it is readily accessible. As a result, many NIH enterprise systems and applications as well as those developed by Institutes and Centers (ICs) use NED data.

Benefits

By providing a convenient, single, logical source of identity and locator information, NED eliminates the need for application-specific repositories of people data, thus reducing the cost of

application development and maintenance. This also reduces the amount of redundant data entry, since NED provides a single place to update the people data used by many major applications.

Applications utilizing NED data can take advantage of persons deregistered in NED to deactivate accounts and revoke authorizations, thereby improving security. For example, when an individual is deregistered in NED, this initiates the disabling of their ID badge and record in the NIH physical access control system, which revokes their card key door lock access.

Applications can also use the HHS ID number or other linking information kept in NED to find the records belonging to an individual that are maintained by other applications, thus making new uses of the data possible. For example, NIH Login allows users to authenticate using their NIH Active Directory account, and NIH Login–enabled applications such as the NIH Business System (NBS) and the Integrated Time and Attendance System (ITAS) can then use NED to locate an authenticated user's record in the Human Resources Database (HRDB).

NIH Environment

The National Institutes of Health (NIH) is the steward of medical and behavioral research for the United States. It is an Agency under the U.S. Department of Health and Human Services, and is comprised of the Office of the Director and 27 Institutes and Centers (ICs), subdivided into more than **2,400 organizational units** (OUs).

NIH headquarters and most research laboratories are located on the main campus in Bethesda, Maryland. The NIH also has facilities in the Rockville, Maryland area and at:

- the NCI Frederick Cancer Research and Development Center (FCRDC) at Fort Detrick in Frederick, Maryland;
- the National Institute of Environmental Health Sciences' main facility in Research Triangle Park (RTP), North Carolina;
- the NIH Animal Center in Poolesville, Maryland;
- the National Institute on Aging's Gerontology Research Center in Baltimore, Maryland;
- the Division of Intramural Research of the National Institute on Drug Abuse, also in Baltimore;
- the National Institute of Allergy and Infectious Diseases' Rocky Mountain Laboratories in Hamilton, Montana; and,
- smaller field units in Phoenix, Arizona, Boston, Framingham, and Waltham, Massachusetts, Detroit, Michigan, and Jackson, Mississippi.

NED represents over **400 buildings** at these sites that are occupied by a workforce of over **45,000 people**, including 19,000 government employees, 4,200 fellows, 17,000 contractors, and 5,000 volunteers, tenants, and guests.

See the NIH Almanac for further information about the NIH environment.

Chapter 2

If you want to understand today, you have to search yesterday.

Pearl Buck

BACKGROUND

Information Technology Central Committee

In 1996, the NIH Director's Leadership Forum agreed to examine ways to centrally manage selected elements of IT at NIH and appointed an Information Technology Central Committee (ITCC) of senior Institute and Center (IC) representatives to develop specific recommendations for improving the management of NIH' s information technology (IT) resources. In developing its recommendations, the ITCC was asked to review previous work done by many NIH IT committees and forge a consensus on specific actions to be taken in the areas of IT organizational structure, interoperability, and security.

Among the recommendations the ITCC made to the NIH Director in December, 1996, was the development of a "centrally coordinated NIH electronic directory". The ITCC envisioned this directory as coordinating or replacing the separate directories then used for email, personnel, parking, etc., and also implementing "deregistration activities", since the committee recognized that accounts and authorizations for services left active after their owners separated from NIH posed an increasing security risk. The NIH Director delegated the implementation of this and the other ITCC recommendations to the NIH Acting CIO.

Architectural Management Group

In 1994, NIH formed an information technology Architectural Management Group (AMG) consisting of representatives from each of NIH's ICs. The AMG's broad goal was to define a uniformly supported, interoperable, IT architecture that enables NIH users to transparently access and use from their workplaces the platforms, processes, and data they need to do their work.

The NIH Acting CIO charged the AMG to provide strategies for the implementation of the ITCC recommendations, including the electronic directory, in February, 1997.

The AMG's *Report on Interoperability at the NIH* issued in May, 1997, recognized that an electronic directory would require long-term NIH executive commitment and resources, and made the following recommendations:

- Establishment of the NIH centrally-supported electronic directory is a critical priority.
- Development and implementation of the directory is a prerequisite to the emplacement of network security at the NIH.
- The directory must be recognized by all ICs as the authoritative source for directory information.
- Unique personal identifiers (not the Social Security Number) must be defined. This will allow integration with systems based on relational databases.
- Base directory design on both Lightweight Directory Access Protocol (LDAP) and Structured Query Language (SQL) access.
- Declare directory presence a prerequisite for NIH services.
- Establish central directory functional and technical committees.

AMG Technical Subcommittee

The NIH Acting CIO approved the formation of a small Technical Subcommittee, the AMG TSC, to further develop the concept and design of an NIH electronic directory service. The AMG TSC was comprised of technical experts from several ICs plus a consultant hired from The Burton Group (TBG) (now part of Gartner), and met regularly from August, 1997, through November, 1998.

The architecture described in the AMG TSC's final *Architecture Review* issued in November, 1998, included the following features, which were implemented in NED:

- An **NIH ID Number** (now the **HHS ID number**) to uniquely and persistently identify every person represented in the directory
- A **directory schema** defining the data elements (or **attributes**) that describe the people represented in the directory
- A **directory server** to store directory data
- A means to make directory data accessible via the **Structured Query Language** (**SQL**)
- A **meta-directory**, also called a **join engine** (**JE**), to **synchronize** directory data with other repositories of people information (this functionality was scaled back over time and fully decommissioned in December 2016)

- **NEDWeb**, a web application used by NIH Administrative Officers to manage directory content (this application is currently known as the NED Portal and is based on Lombardi Teamworks business process management software)

- An **audit trail** to record changes to directory content

The AMG TSC's directory architecture also included the following features, which have not been implemented in NED due to technical, practical, or resource limitations:

- A 4 to 8-digit **Personal Identification Number** (**PIN**) to enable individuals to prove ownership of their HHS ID Numbers

- A hybrid ("rich") **Directory Information Tree** (**DIT**) with organizational and geographical views of people data

- A means for external applications to directly access directory data via the Lightweight Directory Access Protocol (**LDAP**)

- **Exception reports** to notify NIH Administrative Officers of differences between directory data and that in other repositories

NIH Identification Number

One of the first issues addressed by the AMG TSC was the design of an NIH Unique Identifier (UID) that would be used to reliably associate with an individual all the related information stored in the electronic directory and various other NIH systems and databases. After considering many alternatives and surveying practices at other organizations, the AMG TSC recommended a 10-digit NIH ID[1] number with the following characteristics:

- SCOPE: An NIH ID will be assigned to every individual registered in the NIH electronic directory.

- UNIQUENESS: No two individuals will be assigned the same NIH ID number.

- SINGULARITY: An individual will not be assigned more than one NIH ID number.

- PERSISTENCE: An individual will have the same NIH ID number throughout their entire career.

[1] The NIH ID is now assigned as the HHS ID by the HHS Smart Card Management System (SCMS) using the same standard developed by NIH.

- FORM: The NIH ID number will be a 10-digit decimal number displayed in the form *ddd-dddd-ddc*, for example, 001-0147-906. The rightmost digit will be a check digit[2] computed from the other nine digits.

The AMG adopted this recommendation at their quarterly meeting on October 15, 1997. This has been adopted as NIHRFC 005.

Beginning in 2008, the HHS Identity Management System (IDMS) starting assigning the unique identifier described above, now called the HHS ID number. (NED obtains this number from the HHS IDMS when a NED portal user registers a new person in NED.)

Privacy Act Clearance

Soon after it began meeting, the AMG TSC realized that individual identifying information, such as the SSN and date and place of birth, would need to be collected in order to make HHS ID numbers unique and persistent. Before collecting such information, NED needed to be established as a new system of records and a Privacy Act clearance obtained. The NED Project Team began this process in October, 1997, and the *NED System of Records and Privacy Act Clearance* became effective on May 24, 2000.

Data Server Surveys

From July, 1998, through November, 1999, the NED Project Team surveyed the major NIH-wide databases and associated business processes in order to determine what would be necessary to connect them to the NED meta-directory. The NED Project Team prepared a *Data Server Survey Form* based on one used by TBG, met with database owners and administrators to complete the form and obtain access to or samples of the data involved, and analyzed the data.

Generally, the survey and data analysis revealed that:

- No database contained records for all types of workers.
- No database contained most, or even many of the data elements to be included in NED.
- Rarely did any two databases contain a common key, such as the SSN, to make it simple to join records identifying the same individuals.
- Databases and associated business processes were rarely documented.
- The databases driving payroll and visas contained the most complete, accurate, and consistently-coded information, but usually did not contain locator information. They also operate in arrears, which means that the strong identity information they contain

[2] The HHS ID number uses the ISO 7064 MOD 10,11 check digit standard.

is not available in time for "Entrance on Duty" (EoD) day purposes such as issuing ID badges.

- The quality of data in other types of databases was typically poor, suffering from one or more of the following problems: missing/invalid values, inconsistently coded values, old data, records not removed for workers who have left, and duplicate records.
- Database technology and associated business processes did not change often. Most systems were at least 10 years old, and two about 20 years old.
- No single, complete, up-to-date sources for building and organization information existed.

In short, utilizing existing data and business processes to construct NED was going to be more of a challenge than anyone anticipated.

Directory Technology Assessment

As the AMG TSC's directory architecture neared completion, it commissioned TBG to assess commercially available directory and meta-directory products and services. Vendors considered included ISOCOR, Zoomit, Control Data Systems, Open Directory, and Netscape. As reported in the *NED Technology Assessment*, TBG determined that ISOCOR and Zoomit had the most suitable offerings.

The NED Project Team acquired evaluation copies of the Zoomit VIA and ISOCOR MetaConnect meta-directory products in late 1998, conducted proof-of-concept testing, and chose MetaConnect, even though it was still in beta test. MetaConnect had a more flexible architecture, better support for event-driven operation, and could be easily extended with customer-supplied Perl scripts rather than Zoomit's proprietary language.

Critical Path (CP) acquired ISOCOR[3] in October, 1999. CIT purchased MetaConnect late in 1999 after it became generally available, and also purchased CP's X.500/LDAP Global Directory Server (GDS).

Directory Steering Committee

The Directory Steering Committee (DSC) was established in February, 1999, to work with the NED Project Team to identify system requirements and address the many implementation issues associated with a project of this scope. Composed primarily of NIH Administrative Officers (AOs) from representative ICs, the DSC met on a biweekly basis through October 1999 to consider issues

[3] AOL/Netscape licensed the MetaConnect version 1 source code from ISOCOR in January, 1999, and the resulting product came to be sold by Sun Microsystems as Netscape Metadirectory Services. Microsoft acquired Zoomit in July, 1999, and evolved their Via product into the Microsoft Identity Integration Server (MIIS). Novell partnered with ISOCOR in developing an NDS eDirectory connector for MetaConnect until July, 1999, when Novell announced it would develop its own meta-directory product, dirXML, which became generally available in July, 2000. Due to the influence of the partnership, dirXML (now known as Nsure Identity Manager) offers functionality similar to that of MetaConnect.

such as user interface design, security and Privacy Act considerations, business processes, potential uses of NED, and community education and outreach.

The DSC and the NED Project Team engaged in joint design and development of NEDWeb, the web application AOs and Administrative Technicians (ATs) use to register, update, and deregister entries in NED for the individuals for whom they are responsible. The major areas the DSC addressed included:

- data elements to include in NED, and from where to obtain them,
- authoritative sources for IC and other data elements,
- organizational and person status classifications,
- AO/AT authorization control and workflow,
- process for reassigning an individual to a different IC,
- design of the NEDWeb user interface, and
- data sources and strategy for "seeding" the NED database

The DSC and the NED Project Team also developed a plan for conducting a NEDWeb pilot test.

NEDWeb Pilot Test and Deployment

Concurrently with NEDWeb design and development, the NED Project Team developed **connectors** to the seven data sources[4] used to initially populate the NED database. Connectors are software components that read source data and prepare it for matching and loading into the meta-directory. Though designed for compatibility with the selected MetaConnect product, the connectors were run stand-alone to load NED database tables in Oracle since the MetaConnect product was still in beta test, and not yet generally available.

To identify all records in the source databases that referred to the same individual, the NED Project Team adapted software and methodology developed by the U. S. Bureau of the Census Statistical Research Division for performing **probabilistic record linking**. This process generated an HHS ID number for each person and assigned it to all linked records, thus allowing them to be joined and their data elements merged into a single record per person in the NED test database.

The NEDWeb pilot test began in November, 1999. After attending trial training sessions developed and conducted by the NED Project Team, AOs and ATs from CIT, NCRR, NHLBI, NIAA, and NINR used NEDWeb to perform simulated work on the test database. Feedback from the pilot test resulted in many improvements and corrections for problems.

[4] HRDB, Fellowship Payment System (FPS), JEFIC, Parking and ID Badge system (PAID), Integrated Time and Attendance System (ITAS), and NIH Telephone Directory.

When the NED System of Records and Privacy Act Clearance became effective in May 2000, the NED Project Team reinitialized the NED database with fresh data from the seven sources, and production use of NEDWeb began. By August, 2000, NEDWeb was successfully deployed to all ICs except NIEHS[5].

NIH ID Badge and Card Access System

Fortuitously, the NIH Division of Public Safety (DPS) (now a part of the NIH Division of Personnel Security and Access Control (DPSAC)) began preparing in 1998 to replace NIH's outdated ID badge and card access systems, including replacing all card access readers installed on the NIH Bethesda campus and reissuing 25,000 ID badges. This created the opportunity to integrate NED with the new Andover Controls *Continuum* access control system.

The NED Project Team and DPS staff began meeting in December, 1999, to determine requirements and agree upon the NED/Continuum interface specification. The interface was subsequently developed, successfully tested in October, 2000, and deployed in December, 2001, to support the campus-wide rebadging effort, which began in January, 2002.

Due to Homeland Security Presidential Directive 12 which called for the establishment of a uniform Federal identification badge, the NIH ID badging processes were revamped in October 2008 to meet the specifications of the NIST FIPS 201 standard for the personal Identity Verification (PIV) badges. To do this, Lombardi Teamworks (now IBM WebSphere Lombardi Edition) was purchased and became the business process management software making up the NEDWeb portion of the NED system.

Meta-Directory Development and Deployment

Development of the NED meta-directory based on Critical Path MetaConnect v2.1 and GDS v3.0 products began in February, 2000. This involved:

- installing and configuring the LDAP directory server with the schema developed by the AMG TSC,
- integrating the connectors and probabilistic record linking software developed for the pilot test with the meta-directory,
- developing new connections to the NEDWeb-maintained production database, the new NIH ID Badge and Card Access system, and NIH Telephone Directory, and
- programming the meta-directory to flow the dozens of data elements among these connected repositories as determined by the data server surveys and the DSC.

[5] NIEHS AOs continued to use their own directory database and content management web application until mid-2002, when they began using NEDWeb. Until then, the only means provided for managing NIEHS people in NED was the meta-directory, which began auto-registering/deregistering NIEHS Employees and Fellows and updating their locator information via PH in November, 2001.

The NED Project Team immediately encountered serious defects in both GDS and MetaConnect. CP resolved these sufficiently by June so that the software was usable; however, subsequent releases introduced new problems which CP did not resolve, so both products effectively became unsupported. Development proceeded only by working around problems as they were discovered.

The meta-directory was deployed in November, 2001, with connections to the four payroll/visa systems and the email directory[6]. Connections to the new NIH ID Badge and Card Access system and NIH Telephone Directory and were added in December, to the NIH Library Patron Database in April, 2002, and to DB2 on OS/390 in May, 2002.

NIH Login

CIT began the NIH Login project in July, 2002, to provide a single authentication mechanism for NIH Web applications, particularly NBRSS, which was due to go into production in March, 2003.

NIH Login uses Netegrity *SiteMinder* to manage access to web applications and NIH Active Directory (AD) to perform the actual authentication of a user's account name and password. Upon successful authentication, SiteMinder supplies the user's account name to the web applications to which it controls access. NED's role is to enable these applications to use the authenticated account name to find the account owner's NED entry, which is required by applications such as NBRSS and ITAS.

To accomplish this, NED needed to read the account names and other information from over 35,000 AD entries spread across 19 AD domains, match these to NED records, and write them to the DB2 NED table on OS/390. The NED Project Team developed several stand-alone Perl scripts to temporarily perform these synchronization functions once per day, since an AD connector was not available for MetaConnect v2.1. These were deployed for production use in September, 2002.

NIH Login was deployed for production use in September, 2003, and NEDWeb became NIH Login-enabled in January, 2004.

Meta-Directory Upgrade

Due to lack of support from the vendor for GDS v3.0 and MetaConnect v2.1, the NED Project Team declared a moratorium on making additional enhancements to the NED meta-directory and began working in February, 2002, on upgrading to the latest versions of these CP products: InJoin Directory Server (IDS) v4.0 and InJoin Meta-Directory (IMD) v3.4. The upgrade was a major undertaking because:

- the meta-directory application program interface (API) had changed, requiring extensive changes to the NED connectors;

[6] HRDB, FPS, FPS2, JEFIC, and NIH Email Directory and Forwarding Service (PH)

- v2.1 defects had been fixed, allowing most work-arounds to be removed from the NED software;
- new meta-directory features enabled the NED software to be simplified;
- correcting design problems and taking advantage of new features necessitated changes to directory and Oracle database structures, so the upgrade involved migrating and transforming NED production data; and,
- many serious defects were discovered in IMD, including inadvertent removal of v2.1 functionality which NED required.

Fortunately, the new version of the meta-directory software included better diagnostic tools, and CP provided good support and resolved product problems in a timely manner. The NED Project Team shut down NED for a weekend and successfully performed the upgrade in November, 2003. Once again running supported software, it was possible to add new connections, so a connection to the Integrated Time and Attendance System (ITAS) was deployed in March, 2004.

NED Corrective Action Plan (NED CAP)

In 2008 NED management implemented a corrective action plan to fix some shortcomings of the NED system. These included:

- Modernize the core system infrastructure
- Create a scalable architecture that can easily accommodate future NIH needs
- Comply with Federal, DHHS, and NIH security policies and regulations
- Improve overall NED system performance
- Adhere with NIH Enterprise Architecture standards
- Reduce the current workload on operations and maintenance staff

As part of this plan, OD/OCIO determined that NED would become part of an enterprise architecture that promotes the reuse and more flexible data services at the enterprise level. Customers would no longer be "pushed" data but would use enterprise services to fetch the data they needed without having to know where the data came from. This change to how NED services data customers meant no longer needing the CP Meta-directory technology to synchronize copies of data between systems or to link records between different systems.

Meta-Directory Decommissioning

As a goal of the NED CAP was to decommission the CP Meta-Directory software that automatically joins and synchronizes data from and to NIH systems outside of NED. This would

happen piecemeal by shutting down individual connectors after first finding a replacement for the connector functionality.

In April 2012, the NED team be decommissioned the connector supplying NED data to the DB2 NED table on OS/390. All customers using DB2 NED tables reprogrammed their applications to obtain NED data via CIT-supported NED web services, nVision or the NED Oracle data service.

In July 2012, the NED team decommissioned connectors to the J. E. Fogarty Database of Visiting Fellows and Scientists (JEFIC) databases. Data that was in place as of the connector decommissioning was left in place in NED as it was last synched from those sources.

By the end of 2013, the NED Team had decommissioned all meta-directory connections except for HRDB and FPS2. The NED Team decommissioned the HRDB and FPS2 connections in December 2016 and the NED system no longer supports CP Meta-Directory resources.

Chapter

3

A little inaccuracy sometimes saves a ton of explanation.

H. H. Munro (Saki)

FUNCTIONAL OVERVIEW

As described in the Introduction, NED manages identity, organizational, and locator information for all NIH workers. Identity information--distinctive information about an individual that never or rarely changes--includes legal name, gender, date of birth, place of birth, ID badge photo, and other information protected by the Privacy Act. The name of the organization sponsoring an individual and their classification (Employee, Fellow, Contractor, Tenant, Volunteer, or Guest) are the main elements of organizational information. Locator information consists of home and work telephone numbers, building addresses, email addresses, and so forth.

NED Workflow Application

NED collects the bulk of its information via the NED Portal, the user interface component of the NED workflow application, a highly customized implementation of the Lombardi Teamworks business process management (BPM) software. IBM acquired Lombardi several years ago and rebranded the software "IBM BPM". The NED Team expects to migrate the workflow application to IBM BPM by the end of July 2016. The NED Portal supports the following user roles:

- Administrative Officer (AO). AOs have the ability to register new NIH staff in NED and deactivate their records upon separation from NIH, update records, and request NIH services such as ID badges, AD accounts, VPN remote access, NIH Library services, parking, etc. AOs also review and approve AT (see below) requests. AOs have access to data identified as sensitive under the Privacy Act NED System of Records Notice (SORN) for individuals within their scope of authority.

- Administrative Technician (AT). ATs can perform most of the same NED tasks as AOs, but AOs must approve all AT-initiated actions. Thus, ATs lack the ability to change NED data on their own. ATs initiate tasks to register people in NED and

deactivate them when they leave NIH, update records, and request NIH services such as ID badges, AD accounts, VPN remote access, NIH Library services, parking, etc. NED routes AT-initiated tasks to AOs for review and if approved, NED records the update in the database or in the case of a work flow process, advances the task. ATs have access to data identified as sensitive under the Privacy Act NED System of Records Notice (SORN) for individuals within their scope of authority.

- Sponsor. Sponsors are responsible for "substantiating the need" for ID badges and NIH network ("Active Directory") accounts. An AO without the sponsor role can approve ID badge and account requests, but NED ID badge and network processes do not advance until a sponsor approves. Sponsors also perform annual network account reviews in NED to substantiate the need for continued use of the account. NED requires a sponsor to authenticate with a PIV card in order to sponsor ID badges and network accounts.

- Red Parking Approver. NED red parking approvers are able to authorize staff in their IC for a red parking permit.

- Personal Security. Users with the personnel security role have read only access to information contained in all active NED records including some information identified as sensitive under the Privacy Act NED System of Records Notice (SORN). The ORS/Office of Personnel Security director authorizes staff for this role based on a need to access this information to perform official job duties such as determining personnel suitability and conducting background investigations.

- Access Control. Access control users have read only access to miscellaneous non-sensitive NED data such as work contact information, badge tracking, and ID badge status (e.g., authorized or issued). Access to this information assists this group in performing duties centered on the issuance of ID badges.

- Division of International Services (DIS). DIS users have read only access to data contained in active NED records for non-US citizens ("foreign nationals") including data identified as sensitive under the Privacy Act NED System of Records Notice (SORN) such as SSN, date and place of birth, and personal contact information. DIS staff requires this information to perform official job duties involving the determination of foreign nationals' suitability for working at NIH. DIS users can update several NED fields for foreign nationals including legal name, country of citizenship, legal permanent resident status, alien file number, alien authorized to work until date, and date entered U.S. A NED user with the DIS role must also validate a foreign national's work credentials before the foreign national can receive an ID badge.

- NIH IT Service Desk. IT Service Desk users can view non-sensitive NED data and provision and de-provision VPN remote access for NIH Staff.

- ETD Coordinator. Emergency Tier Designation (ETD) Coordinators can view non-sensitive work information and update the ETD of NIH employees affiliated with the coordinator's IC.

- Self-Service. All NIH staff with an Active Directory (AD) account have the NED self-service user role that allows them to view information contained in their own NED record and update certain fields. AOs must approve self-service requests to update other fields. For example, a self-service user can update their work and personal contact and location information without AO approval, but an AO must approve a change to their legal name. A self-service user can also select the personal contact information that NED will make available to the AlertNIH communication system that notifies NIH staff of emergencies and other critical events.

- NIH Support. Various members of the NED team hold the NIH Support role allowing them to perform system support-related functions such as reading and updating data in the HHS Smart Card Management System (SCMS) and the NIH Background Investigation System (BITS), managing in-flight workflow application processes, and viewing in-flight task data.

NED Public Search

NED public search (http://ned.nih.gov) is an online NIH staff directory that displays non-sensitive information on the Internet and NIH intranet. The information displayed includes organization, contact, and locator information, but public search displays less information to customers accessing the application via the Internet than if access is via a computer connected to the NIH intranet. NIH intranet customers include all NIH personnel with NIH network accounts. Internet customers include anyone with Web access.

NED/AD Link Editor Application

NIH IT Service Desk staff in the accounts group use NED/AD Link Editor to manage NIH network (Active Directory) accounts and primary SMTP email addresses. Specifically, the application lets Service Desk staff associate a person's NED record with a different network account username, change their primary SMTP email address, and authorize or de-authorize a network account or Exchange mailbox. The application does not provide access to sensitive NED data. NIH IT Service Desk managers authorize staff for the application and authentication is via NIH Login.

PIV Sponsor Management Application

ORS Division of Personnel Security and Access Control (DPSAC) staff use the PIV Sponsor Management application to manage the NED sponsor role. The application allows users to grant and remove the NED Sponsor role to an NIH FTE who already has the NED AO role following

completion of PIV Sponsor training. DPSAC management authorizes staff for the application and authentication if via NIH Login.

External Data Sources

As described above (see NED Workflow Application), NIH administrative staff with the NED Administrative Officer (AO) and Administrative Technician (AT) roles are responsible for entering and updating much of the information in NED using the NED Portal, but NED receives data from several external date sources.

nVision Organization Data. NED obtains official NIH organizations as recognized by the Department of Health and Human Services (HHS) from nVision daily via an Oracle stored procedure-based batch update process and writes to data to its own internal organization database tables.

Mail Stop Data. NED obtains mail stop data weekly via a Windows service batch process that reads from an OD/Office of Research Services (ORS) MS SQL database and then writes to the NED Oracle database. NED uses the mail stop data to populate a lookup list in the NED Portal.

Active Directory (AD) Data. NED obtains AD primary account data for use in supporting its account-related business processes via a daily batch process. For example, NED uses AD's "password last changed date" to de-authorize accounts when users fail to change their password as required by the NIH Account Life Cycle policy.

Username Data. NED obtains a person's Active Directory user logon name ("samAccountName") from the Uninames database when an Administrative Officer (AO) initially registers the person in NED. The Uninames database resides on a Microsoft SQL Server database supported by the CIT/IAM (Identity and Access Management) group.

Workflow Process Data. The NED workflow application receives web service notifications relating to ID badge and network (Active Directory) account provisioning processes from the HHS Smart Card Management System (SCMS), the NIH Background Investigation Tracking System (BITS), and the NIH Security Awareness Training System (SATS). For example, NED does not authorize ID badge issuance until BITS notifies NED that NIH Personnel Security has adjudicated an applicant's fingerprints. Also, NED does not authorize an NIH network account before SATS indicates the applicant has completed their required security and privacy awareness training.

Support for NIH Business Functions

NED supports a number of important NIH business functions either directly through the NED workflow application or indirectly by supplying validated and normalized data to dozens of downstream systems and applications.

On Boarding / Off Boarding

NED orchestrates the assignment of a single, unique, persistent 10-digit HHS ID number to all NIH staff requiring NIH logical account access or physical access to NIH facilities by transmitting personal identifying information entered in the NED Portal during registration to the HHS Smart Card Management System (SCMS). The SCMS assigns an HHS ID number and provides to NED via its web services interface. NED stores the HHS ID number and propagates to downstream systems and applications for use as a common key in joining records across disparate NIH and HHS systems.

NED facilitates the NIH background investigation and personnel suitability processes through its collection of positon information for new staff and assignment of the appropriate position sensitivity level. NED transmits this information to the Background Investigation Tracking System (BITS) used by the ORS Division of Personnel Security and Access Control (DPSAC) to initiate and track background investigations. NED interacts with BITS to ensure that DPSAC has performed the requisite employment suitability checks before authorizing ID badge issuance. NED also facilitates ORS/ Division of International Services (DIS) screening of foreign national staff by ensuring DIS has validated foreign nationals' official work documents prior to authorizing ID badge issuance.

Upon separation of staff from NIH, NED facilities the de-provisioning of logical account access and physical access to facilities by initiating the revocation of ID badges, NIH logical accounts, and other NIH services.

ID Badge Provisioning

NED orchestrates the provisioning and de-provisioning of the following types of ID badges for logical account access and physical access to NIH facilities:

- HHS ID Badge (PIV card) – smart card providing both logical and physical access
- NIH RLA badge (issued to short-term staff and foreign nationals) – smart card providing both logical and physical access
- NIH ID ("legacy") Badge – RFID card providing physical access only
- Clinical Center Title Badge - non-RFID card issued to staff working in buildings 10, 10A, and 10-CRC on the NIH Bethesda, MD campus providing a "visual credential" when accessing patient and other restricted areas

NED plays a major role supporting NIH's implementation of Homeland Security Presidential Directive (HSPD)-12, which mandates a government-wide standard for the issuance of secure and reliable forms of identification credentials to Federal employees and contractors to access government facilities and networks. NED interacts directly through its workflow application and web service interfaces with the HHS Smart Card Management System (SCMS) and the NIH Background Investigation Tracking System (BITS) to orchestrate the personal identity verification (PIV) process outlined in Federal Information Processing Standard (FIPS) Publication 201-2.

NED interacts with the NIH Physical Access Control Information System (PACSIS) via NIH enterprise web services and the HHS SCMS to authorize ID badges and initiate revocation when NED de-authorizes such credentials. NIH PACSIS also notifies NED when NIH Access Control issues badges so NED can close out workflow application badge processes and display badge tracking information to customers via the NED portal.

NIH Network Account and Email Provisioning

NED orchestrates the provisioning and de-provisioning of NIH network (Active Directory) accounts and mailboxes to staff requiring NIH computer network access in accordance with *NIH Account Life Cycle Policy* guidelines:

- Enforces the completion of mandatory security and privacy awareness training prior to establishing an account and mailbox.
- Enforces the annual review accounts and substantiation of a continued need for an account and mailbox.
- Enforces the requirement that an account holder regularly change their account password.
- Enforces the de-provisioning of an account and mailbox when the account holder separates from NIH.

Teleworking and Remote Access

NED provisions and de-provisions NIH Virtual Private Network (VPN) remote access to support teleworking and access to NIH computing resources by non-local individuals conducting official NIH business.

NIH Parking and Transhare

NED authorizes and de-authorizes the issuance of NIH parking hangers and supplies data to the ORS Division of Amenities and Transportation Services (DATS) Commuting and Parking Services (CAPS) system that determines eligibility for parking privileges and the NIH Transhare program.

NIH Library Services

NED authorizes and de-authorizes access to NIH Library services and resources.

NIH Telephone Directory and Operator Services

NED provides staff locator and telephone data to the NIH Telephone Operators Database and authorizes and de-authorizes listing in the printed NIH Telephone and Services Directory.

NIH Emergency Preparedness

NED supports the mission of the ORS Division of Emergency Preparedness and Coordination (DEPC) and Office of Human Resources (OHR):

- Collects and manages NIH employee emergency tier designations (ETDs) and makes this information available to external systems including nVision for reporting purposes.

- Provides work and personal contact information to DEPC's SendWordNow system, which underpins the AlertNIH managed communication system that is responsible for notifying staff of emergencies, office closings, and other time-sensitive information.

- Provides a web interface for NIH staff to select which personal contact information NED makes available to SendWordNow.

NIH Staff Directory

NED public search (http://ned.nih.gov) provides the official NIH staff directory of location and work information to NIH internal staff and the general public via the Web.

NIH Annual Census

The NIH Office of Research Facilities (ORF) uses NED data as the basis for its annual census used to calculate space utilization rates and allocate $300M in central services costs to ICs.

Data Broker

NED provides data to dozens of downstream NIH and HHS systems and applications ("data customers") that utilize the data in support of a wide variety of business processes. Customers obtain NED data via the following methods:

1. nVision NED Repository. nVision obtains NED data via a daily (Monday-Friday) ETL process and provides customers SQL access to the data via several nVision Oracle database tables.

2. NIH enterprise web services. NED makes data available via several enterprise web services that allow customers to receive near real-time access to NED data and notifications of record updates.

3. NED Oracle data services (not available to new customers). Systems and applications can obtain data directly from the NED Oracle database by calling a customized stored procedure from a package. Management has indicated that these customers should eventually switch to either the nVision NED Repository or NIH enterprise web services for obtaining NED data.

NED data customers include the following systems and applications:

- NIH Business System (NBS)

- Electronic Research Administration (eRA)

- Active Directory Manager (ADM)/Global Address List (GAL)

- Biomedical Translational Research Information System (BTRIS)
- Fellowship Payment System
- Purchase Order Tracking System (POTS)
- Workflow Information Tracking System (WiTS)
- Integrated Time and Attendance System (ITAS)
- HHS Learning Management System (LMS)
- Security and Privacy Awareness Training System (SATS)
- Employee Database Internet Edition (EDIE)
- NIH Physical Access Control Information System (PACSIS)
- ServiceNow (NIH IT Service Desk incident, problem, and change tracking application)
- HHS Employee Directory
- GovTrip
- NIH Enterprise Ethics System (NEES)
- Ethics Management Information System (EMIS)
- NIH Intramural Database (NIDB)
- Helix
- Radiation Safety Database
- NIH Incident Response Team (IRT) Portal
- NIH Security Authorization Tool (NSAT)
- NIH Commuting and Parking Services (CAPS)

NED Physical System Diagram

FIGURE 1 below depicts the physical components of NED and how these connect to the other major systems.

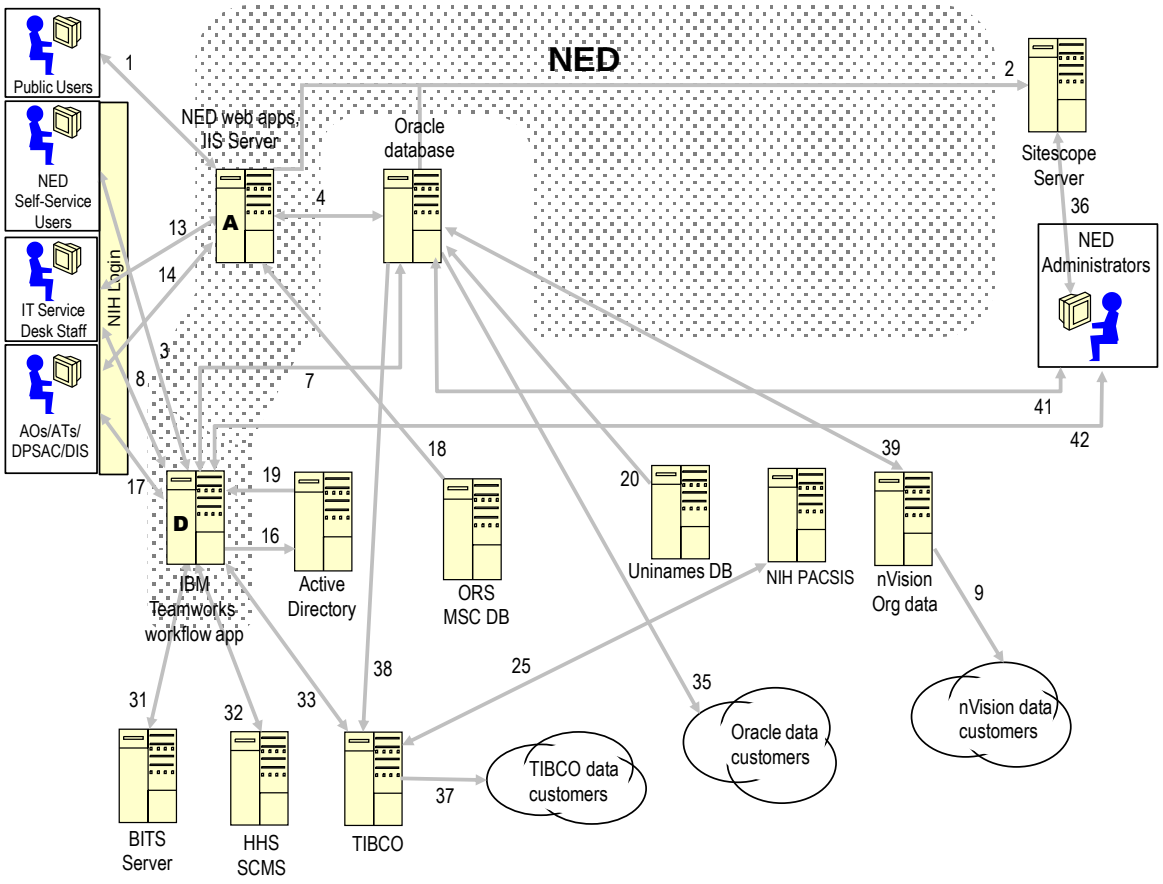

FIGURE 1 NED Physical System Diagram

TABLE 1 NED Connections Summary

Connection Number	Protocol	Purpose
1	HTTP	The general public uses web browsers to communicate with the NED public search application (http://ned.nih.gov) running under Microsoft Internet Information Services (IIS). NED displays a limited amount of information to the public.

Connection Number	Protocol	Purpose
2	Various	Various Sitescope monitors scan NED hardware and software logs to alert the NED team of abnormalities.
3	HTTPS	NED record owners use web browsers to communicate with the IBM Teamworks workflow application. NIH Login controls authentication.
4	Oracle SQL*Net	The NED Public Search, NED/AD Link Editor, NED PIV Sponsor Management applications and the mailstop update process access Oracle database tables.
7	Oracle SQL*Net	The IBM Teamworks workflow application on machine **B** accesses Oracle database tables and stored internal workflow information in Oracle.
8	HTTPS	NIH IT Service Desk staff use web browsers to communicate with the IBM Teamworks workflow application. NIH Login controls authentication.
9	Oracle SQL*Net	NED data customers access nVision Oracle database tables.
13	HTTPS	NIH IT Service Desk staff use web browsers to communicate with the NED/AD Link Editor application running under IIS. This application allows authorized staff to change the NIH Active Directory account name and handle account and mailbox authorizations. NIH Login controls authentication.
14	HTTPS	NIH administrative staff (e.g., AOs, ATs) and DSPSAC staff use web browsers to communicate with legacy NED web application interfaces running under Microsoft Internet Information Services (IIS). NIH Login controls authentication.
16	LDAP	The IBM Teamworks workflow application updates Active Directory (AD) VPN security groups.
17	HTTPS	NIH administrative staff (e.g., AOs, ATs), DPSAC staff and DIS staff use web browsers to communicate with the IBM Teamworks workflow application. NIH Login controls authentication.

Connection Number	Protocol	Purpose
18	Microsoft SQL Server	The NED mail stop code (MSC) update process reads MSC database managed by ORS.
19	LDAP	The IBM Teamworks workflow application reads entries in the NIH Active Directory (AD) and updates the NED_AD Oracle table.
20	Microsoft SQL Server	The IBM Teamworks workflow application obtains NED NIHSSOUSERNAME data from and registers new users in the UNINAMES Database.
25	Web Services	NIH Integration Services Center web services write/read ID badge and locator data to/from the NIH Physical Access Control Integration System (PACSIS).
31	Web Services	IBM Teamworks workflow application web services write/read background investigation-related data to/from Background Investigation Tracking System (BITS).
32	Web Services	IBM Teamworks workflow application web services write/read identity and smart card-related data to/from the HHS Smart Card Management System (SCMS).
33	Web Services	TIBCO web services notify the IBM Teamworks workflow application of completed NIH security and privacy awareness and remote access user training.
35	Oracle SQL*Net	NED data customers invoke an Oracle stored procedure to read from NED database tables.
36	HTTP	The NED team uses web browsers to communicate with the Sitescope monitor administrative web site.
37	Web Services	NED data customers access TIBCO enterprise services.
38	Oracle SQL*Net	TIBCO enterprise services access the NED Oracle database.
39	Oracle SQL*NET	NED accesses nVision Oracle tables to obtain organizational data. nVision accesses the NED Oracle database to obtain data for used by downstream systems and reporting.

Connection Number	Protocol	Purpose
41	Oracle SQL*Net	Various Oracle administrative and query tools used by NED team to manage Oracle instances and data maintenance tasks for NED.
42	HTTP	The NED team manages uses administrative functions of the IBM Teamworks workflow application on machine **B**.

The following tables describe the configurations of the server machines (labeled A and B in FIGURE 1) for the production, test, and development NED instances.

TABLE 2 NED Production Server Configurations

Machine	Configuration
A	▪ Machine Name: NIHNEDWEBPROD3.NIH.GOV ▪ HP Proliant BL460 G3 ▪ Dual 2.27GHz processors ▪ 4GB physical memory ▪ 36GB and 100GB drives ▪ Microsoft Windows Server 2003 SP2
B	▪ Machine Name: MERLIN.CIT.NIH.GOV ▪ Sun SunFire V445 ▪ Quad UltraSPARC-IIIi 1592 Mhz processors ▪ 24GB memory ▪ 4 146GB disk drives (mirrored - 292GB of usable disk space) ▪ Solaris 10

TABLE 3 NED Test Server Configurations

Machine	Configuration
A	▪ Machine Name: NIHNEDWEBDEV3.NIH.GOV ▪ HP Proliant BL460 G3 ▪ Dual 2.27GHz processors ▪ 4GB physical memory ▪ 36GB and 100GB drives ▪ Microsoft Windows Server 2003 SP2
B	▪ Machine Name: OSPREY.CIT.NIH.GOV ▪ Sun SunFire-V240 ▪ 8 GB physical memory ▪ Dual single core UltraSparc-IIIi 1.5GHz processors ▪ Mirrored 72GB Disk Drives for Boot Drives, Dual 146GB Internal Drives ▪ Solaris 10

Appendix A – NED Functional Interconnection Diagram

FIGURE 2 NED Functional Interconnections Diagram