

**Volume**

**1**

NATIONAL INSTITUTES OF HEALTH

---

NIH Enterprise Directory

# NED Overview

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
		Keith Gorlen	Change title back to NED Overview
	April 30, 2005	Keith Gorlen	Update for Remedy, BITS, and Oracle NED_PERSON_BASE.
	December 27, 2007	Robert Malick	Updated NED physical diagram, hardware configurations, removed PH connector, renamed NHLBI eDirectory to Constellation Provisioning System, and updated some outdated concepts.
	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.
	November 1, 2010	Robert Malick	Updated Figure 1 NED Physical System Diagram and Table 1 NED Connections Summary.
	January 30, 2012	Robert Malick	Updated NED Physical System diagram and summary. Updated many sections.
	May 29, 2012	Robert Malick	Removed references to HRDB, JEFIC and FPS2 systems.
	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

---

Version	Date	Contributors	Summary
			LDAP Directory Server to Oracle. Made corresponding updates to Table 1 (NED Connections Summary).

# 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.....	19
FUNCTIONAL OVERVIEW .....	21
NED Physical System Diagram .....	22
Identity Binding.....	29
Content Management.....	29
ID Badge Provisioning.....	29
NIH Active Directory .....	30
Telephone Directory .....	30
Integrated Time and Attendance System.....	30
NIH Library Patron Database .....	31

**NED OVERVIEW**

Service Desk Customer Database.....	31
FUTURE WORK .....	33
Improve Deregistration .....	33
Manage Organization and Buildings Data .....	33
Index .....	34

## List of Tables

TABLE 1 NED Connections Summary .....	23
TABLE 2 NED Production Server Configurations .....	26
TABLE 3 NED Test Server Configurations .....	28



# List of Figures

FIGURE 1 NED Physical System Diagram..... 23



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, 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, NED is used by many enterprise-wide applications at NIH.

### 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 connected to NED 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 deactivates their record in the ID badge 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 and Research Support System](#) (NBRSS) 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 **2,300 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.

## **N E D O V E R V I E W**

A total of over **340 buildings** at these sites are occupied by a workforce of over **40,000 people**, including 18,000 government employees, 4,000 fellows, 13,000 contractors, and 5,000 tenants, volunteers, and guests.

See the [NIH Almanac](#) for further information about the NIH environment.

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 have been 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

- **NEDWeb**, a web application used by NIH Administrative Officers to manage directory content
- 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<sup>1</sup> 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.

---

<sup>1</sup> 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<sup>2</sup> computed from the other nine digits.

The AMG adopted this recommendation at their quarterly meeting on October 15, 1997. This has been adopted as [NIHREFC 005](#).

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

---

<sup>2</sup> The HHS ID number uses the ISO 7064 MOD 10,11 check digit standard.

- 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<sup>3</sup> 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

---

<sup>3</sup> 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.

consider issues 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<sup>4</sup> 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,

---

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

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.

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<sup>5</sup>.

## **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,

---

<sup>5</sup> 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.

- 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.

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<sup>6</sup>. 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

---

<sup>6</sup> HRDB, FPS, FPS2, JEFIC, and NIH Email Directory and Forwarding Service (PH)

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;
- 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, it was deemed 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 that is 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 the CP Meta-Directory software that automatically joins and synchronizes data from and to NIH systems outside of NED would be decommissioned. This would happen piecemeal by shutting down individual connectors after first finding a replacement for the connector functionality.

In April 2012 the first connector to be decommissioned was 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 June 2012 the three HR-based connectors retrieving data from HRDB, Fellowship Payment System II (FPS2), and J. E. Fogarty Database of Visiting Fellows and Scientists (JEFIC) databases were decommissioned. Data that was in place as of the connectors decommissioning was left in place in NED as it was last synched from those sources.

Decommissioning of connectors will continue as the databases to which NED supplies data find alternative means of retrieving data from NED. Once all connectors are decommissioned, the CP Meta-Directory resources will no longer be supported as part of the NED system.



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 name, sex, date of birth, place of birth, ID 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 acquires and coordinates identity, organizational, and locator information among other systems and databases, including:

- NIH ID Badge Physical Access Control System (Continuum)
- NIH Active Directory (AD)
- NIH Telephone and Services Directory
- NIH Integrated Time and Attendance System (ITAS)
- NIH Library Patron Database
- NIH Service Desk Customer Database (Remedy)

To accomplish this, NED:

- binds individual identities to HHS ID numbers;
- enables NIH Administrative Officers (AOs) and Administrative Technicians (ATs) to register, update, and deactivate records for NIH workers;

## **NED OVERVIEW**

- enables individuals to update their own records;
- connects to other systems and databases via a wide variety of protocols and interfaces;
- parses, validates, and standardizes about 80 identity and locator data elements;
- finds and links records that identify the same individual;
- selects and merges all data elements for an individual into a single meta-directory record; and,
- creates, updates, and deletes records in connected systems in response to external events, as determined by nearly 1,000 custom business rules.

The result is that NED and all systems and databases to which it is connected contain up-to-date, consistent, standardized identity, organizational, and locator information for the entire NIH workforce.

### **NED Physical System Diagram**

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

**NED OVERVIEW**

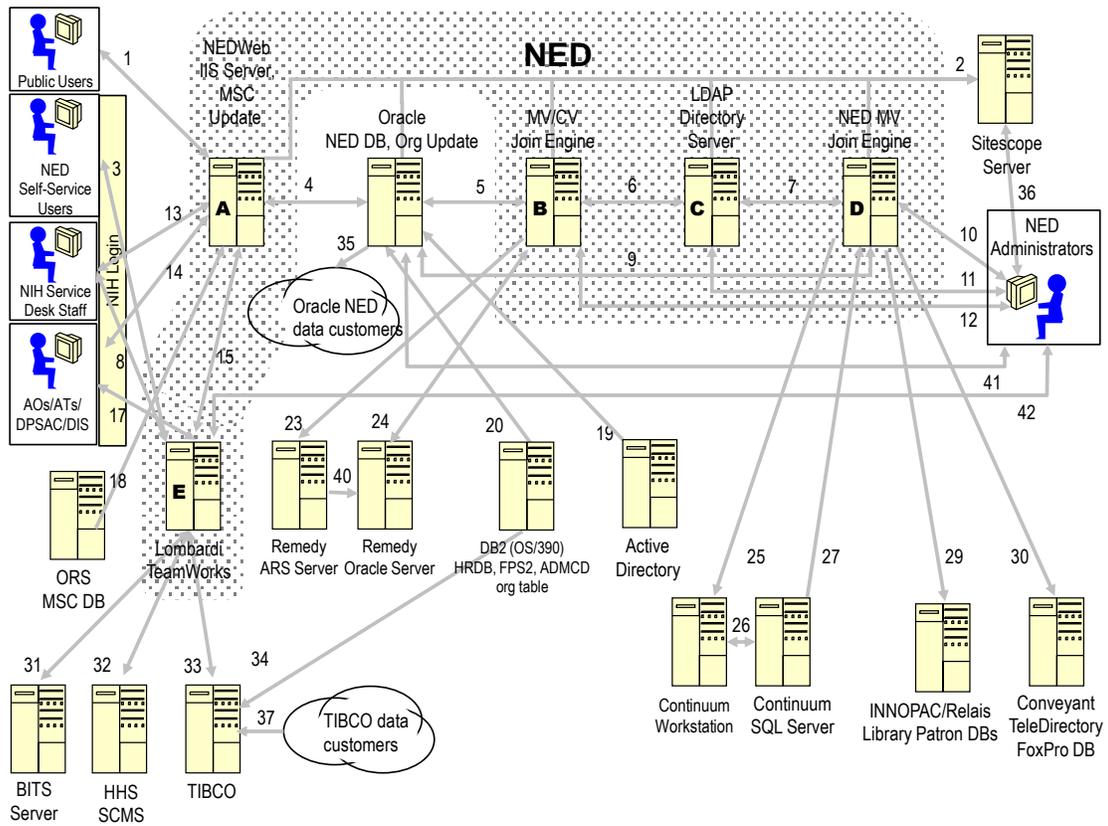


FIGURE 1 NED Physical System Diagram

TABLE 1 describes the numbered connections shown in Figure 1.

TABLE 1 NED Connections Summary

Connection Number	Protocol	Purpose
1	HTTP	Web browsers used by the public communicate with NEDWeb search application running under Microsoft Internet Information Services (IIS). The public is curtailed from seeing all available NED data.
2	Various	Various Sitescope monitors scan NED hardware and software logs to alert NED staff of abnormalities.
3	HTTPS	Web browsers communicate with Lombardi TeamWorks workflow application. Authentication is controlled by NIH Login.
4	Oracle	NEDWeb, NED Link Editor, and mailstop update tasks access

Connection Number	Protocol	Purpose
	SQL*Net	Oracle database tables.
5	Oracle SQL*Net	Critical Path™ Meta-Directory Server (JE) on machine <b>B</b> accesses Oracle database tables.
6	LDAP	Critical Path™ Meta-Directory Server (JE) on machine <b>B</b> accesses Critical Path™ Directory Server on machine <b>C</b> .
7	LDAP	Critical Path™ Meta-Directory Server (JE) on machine <b>D</b> accesses Critical Path™ Directory Server on machine <b>C</b> .
8	HTTPS	Web browsers used by NIH Service desk staff communicate with Lombardi Teamworks workflow application. Authentication is controlled by NIH Login.
9	Oracle SQL*Net	Critical Path™ Meta-Directory Server (JE) on machine <b>D</b> accesses Oracle database tables shared with NEDWeb, and the Oracle NED_PERSON_BASE table read by external applications.
10	Telnet	Critical Path™ Management Center used by NED team to manage Critical Path™ Meta-Directory Server (JE) on machine <b>D</b> .
11	LDAP	Critical Path™ Management Center used by NED team to manage entries on Critical Path™ Directory Server on machine <b>C</b> and the Critical Path™ Meta-Directory Server configuration for machines <b>D</b> and <b>B</b> .
12	Telnet	Critical Path™ Management Center used by NED team to manage Critical Path™ Meta-Directory Server (JE) on machine <b>B</b> .
13	HTTPS	Web browsers used by NIH Service desk staff communicate with AD/NED 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. Authentication is controlled by NIH Login.
14	HTTPS	Web browsers used by AOs and ATs communicate with legacy NEDWeb application interfaces running under Microsoft Internet Information Services (IIS). Authentication is controlled by NIH Login.

**NED OVERVIEW**

<b>Connection Number</b>	<b>Protocol</b>	<b>Purpose</b>
15	Oracle SQL*Net	Lombardi TeamWorks workflow application on machine <b>E</b> accesses Oracle database tables and stored internal workflow information in Oracle.
17	HTTPS	Web browsers used by AOs, ATs, DPSAC staff and DIS staff, communicate with Lombardi Teamworks workflow application. Authentication is controlled by NIH Login.
18	Microsoft SQL Server	Mail stop code (MSC) update task reads MSC database managed by ORS.
19	LDAP	NED LDAP AP Java Connector reads entries in NIH Active Directory (AD) and updates an AD reference table in Oracle.
20	IBM DB2	JE connectors obtain HRDB and FPS2 data changes and organizational code update task reads HRDB DB2 tables via the Oracle database server and the Oracle Transparent Gateway to DB2.
23	ARS	HELPCConnect custom JE Perl connector writes data to the NIH Service Desk customer database via the Remedy ARS Server CIT Customer Database form.
24	Oracle SQL*Net	HELPCConnect custom JE Perl connector reads data from the NIH Service Desk customer database.
25	CIFS	Continuum Personnel Data Import (PDI) application reads NED data and commands from files written by ONEIDConnect custom JE Perl connector from shared folder on machine <b>D</b> .
26	Microsoft SQL Server	Continuum Personnel Data Import (PDI) application reads/writes data to Continuum database.
27	Microsoft SQL Server	ONEIDConnect custom JE Perl connector reads NIH ID Badge Physical Access Control System database tables.
29	CIFS	NIH Library Innopac and Relais applications read NED data files written by CCLIBConnect custom JE Perl connector from shared folder on machine <b>D</b> .
30	CIFS	Conveyant TeleDirectory host interface (hostif) application reads NED data and commands from files written by OPERConnect custom JE Perl connector to shared folder on

Connection Number	Protocol	Purpose
		machine <b>D</b> .
31	Web Services	TeamWorks web services writes/reads to/from Background Investigation and Tracking System (BITS) background investigation related data.
32	Web Services	TeamWorks web services writes/reads to/from HHS Smart Card Management System (SCMS) PIV card related data.
33	Web Services	TeamWorks web services writes/reads to/from Integration Services Center TIBCO software for details about security training and ISSO remote access authorization from the Security Access Training System (SATS).
34	IBM DB2	Integration Services Center TIBCO software reads NED DB2 tables to provide web service access to NED data.
35	Oracle SQL*Net	NED Oracle Data Customers read NED Oracle tables.
36	HTTP	Web browsers used by the NED staff to communicate with Sitescope monitor administrative web site.
37	Web Services	Integration Services Center TIBCO data customers read from TIBCO NED web services.
40	Oracle SQL*Net	Remedy ARS server writes NED data changes to the NIH Service Desk customer database.
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	NED team uses administrative functions of the Lombardi TeamWorks application to manage Lombardi TeamWorks workflow application on machine <b>E</b> .

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

TABLE 2 NED Production Server Configurations

<b>Machine</b>	<b>Configuration</b>
A	<ul style="list-style-type: none"> <li>▪ Proliant BL20p G3</li> <li>▪ 2 3600MHz Intel Xeon CPUs</li> <li>▪ 2GB physical memory</li> <li>▪ Mirrored 69460MB disk drives</li> <li>▪ Microsoft Windows Server 2003 SE SP2</li> </ul>
B	<ul style="list-style-type: none"> <li>▪ Proliant BL20p G3</li> <li>▪ Dual 3600MHz Intel Xeon processors</li> <li>▪ 2GB physical memory</li> <li>▪ Mirrored 69460MB disk drives</li> <li>▪ Windows Server 2003 SP2</li> </ul>
C	<ul style="list-style-type: none"> <li>▪ SunFire V240</li> <li>▪ Dual UltraSPARC-IIIi 1503 Mhz processors</li> <li>▪ 8GB memory</li> <li>▪ 4 internal disk drives (2 72GB mirrored, 2 146GB mirrored)</li> <li>▪ Solaris 9</li> </ul>
D	<ul style="list-style-type: none"> <li>▪ Proliant BL20p G3</li> <li>▪ Dual 3600MHz Intel Xeon processors</li> <li>▪ 2GB physical memory</li> <li>▪ Mirrored 140010MB disk drives</li> <li>▪ Windows Server 2003 SP2</li> </ul>
E	<ul style="list-style-type: none"> <li>▪ SunFire V445</li> <li>▪ Quad UltraSPARC-IIIi 1592 Mhz processors</li> <li>▪ 24GB memory</li> </ul>

Machine	Configuration
	<ul style="list-style-type: none"> <li>▪ 4 146GB disk drives (mirrored - 292GB of usable disk space)</li> <li>▪ Solaris 10</li> </ul>

TABLE 3 NED Test Server Configurations

Machine	Configuration
A	<ul style="list-style-type: none"> <li>▪ Proliant BL20p G3</li> <li>▪ 2 3600MHz Intel Xeon CPUs</li> <li>▪ 2GB physical memory</li> <li>▪ Mirrored 69460MB disk drives</li> <li>▪ Microsoft Windows Server 2003 SE SP2</li> </ul>
B	<ul style="list-style-type: none"> <li>▪ Proliant BL20p G3</li> <li>▪ Dual 3600MHz Intel Xeon processors</li> <li>▪ 2GB physical memory</li> <li>▪ Mirrored 69460MB disk drives</li> <li>▪ Windows Server 2003 SP2</li> </ul>
C	<ul style="list-style-type: none"> <li>▪ Sunfire v240</li> <li>▪ Dual UltraSPARC-IIIi 1280MHz processors</li> <li>▪ 8GB physical memory</li> <li>▪ 2x146GB disk drives (boot and mirror), 1x72GB disk drives</li> <li>▪ Solaris 9</li> </ul>
D	<ul style="list-style-type: none"> <li>▪ Proliant BL20p G3</li> <li>▪ Dual 3600MHz Intel Xeon processors</li> <li>▪ 2GB physical memory</li> </ul>

Machine	Configuration
	<ul style="list-style-type: none"> <li>▪ Mirrored 69460MB disk drives</li> <li>▪ Windows Server 2003 SP2</li> </ul>
E	<ul style="list-style-type: none"> <li>▪ Sun-Fire-V240</li> <li>▪ 8 GB physical memory</li> <li>▪ 2 CPUs</li> <li>▪ Mirrored 72GB Disk Drives for Boot Drives, Dual 146GB Internal Drives</li> <li>▪ Solaris 10</li> </ul>

## Identity Binding

**Identity binding** is the process of assigning a single, unique, persistent HHS ID number to each individual identity in NED. The NEDWeb application does this when AOs register people and the HHS SCMS assigns or reassigns an HHS ID to the identity information.

## Content Management

The NEDWeb application is also the primary means of performing **content management**: adding, updating, and deleting entries for people in NED. AOs perform all three functions for the people in the organizations they administer, while individuals can view all, but update only a subset of the information in their own NED entries via the NEDWeb Self Service application.

## ID Badge Provisioning

The NIH ID Badge Physical Access Control System is built on the Andover Controls *Continuum* product and operated by the NIH Division of Personnel Security and Access Control. NED **provisions** the ID badge system with records for people; that is, NED is the only means by which ID badges can be authorized, renewed, replaced, and revoked. AOs perform these four badge-related functions for the people in the organizations they administer by using NEDWeb.

The NED JE bidirectionally exchanges data with Continuum. NED sends add, modify, and deactivate commands and the HHS ID number, name, legal name, organizational status (employee type), IC, building, room number, telephone number, and badge title to Continuum. When a PIV badge is issued by DPSAC via a NEDWeb interface, the JE will send the photo it

received from the HHS SCMS with the ID badge number to Continuum. The JE will read a photo from Continuum in the case where the photo was taken for a locally issued NIH badge.

HHS ID badges have the badge holder's HHS ID number printed on the bottom front of the badge, and encoded on a magnetic stripe and barcode on the back. Applications such as the NIH Library Patron Database and Parking and Transhare System read the barcode to determine a user's identity.

When an individual separates from NIH, changes their organizational status from Employee to Contractor, for example, NED deactivates their record in the ID badge system.

## **NIH Active Directory**

Microsoft Active Directory (AD) is an LDAP-accessible directory service used by Microsoft Windows platforms and other applications to store and retrieve information about enterprise resources such as user accounts, computers, printers, and servers. Most importantly, it provides authentication services for Windows and NIH Login, and an address book for Microsoft Exchange 2003 email.

The NIH Active Directory configuration currently consists of a single NED domain with a total of over 40,000 user account entries. NED reads a snapshot of the NIH domain daily for purposes of easy SQL access of the information. A Join Engine AD connector reads AD changes and matches AD user account entries to NED entries, and populates NED entries with AD domain and user account names. In response to trouble calls, the NIH Service desk can manually override the AD domain and user account name associated with an individual's entry in NED to make corrections and to resolve ambiguities—many individuals have multiple AD user accounts.

## **Telephone Directory**

NIH Telephone Operator Services uses the NIH Telephone and Services Directory to manage calls to the NIH main switchboard at 301-496-4000. NED provisions the Personnel Listing ("white pages") portion of this directory, which is based on Conveyant Systems *TeleDirectory*® software product.

A hard-copy version of the Personnel Listing is also published twice each year as part of the *NIH Telephone and Services Directory*. Using NEDWeb, AOs can control whether or not an individual is included in the printed listing.

## **Integrated Time and Attendance System**

NIH employees use the Integrated Time and Attendance System (ITAS) to track and report their work hours and leave, and to view leave and earnings statements.

ITAS is an NIH Login-enabled application which internally identifies employees using their SSN. NED's "live" connection to a table in the ITAS database provides the mapping between NIH AD domain/user account names and employee SSNs as well as provides such items as email address.

## **NIH Library Patron Database**

The NIH Library provides a comprehensive range of scientific, medical, and administrative information and support services to NIH researchers. The library uses Innovative Interfaces' INNOPAC Millennium product to manage information about its patrons, and Relais to deliver documents electronically.

AOs can authorize individuals for library services via NEDWeb. Each day, NED generates an INNOPAC-compatible file containing the name, HHS ID number, organizational, and locator information of all authorized individuals. When checking out materials or using other library services, the patron's HHS ID number is scanned from the barcode on their badge, allowing the library to verify authorization for library services and to contact the patron or their AO when necessary.

The NIH Library also uses the INNOPAC file to update the Relais customer database nightly, allowing electronic fulfillment of document requests by delivery of PDF files containing scanned images of journal articles.

## **Service Desk Customer Database**

The NIH Service Desk Customer Database supports the submission and processing of service request tickets for customer support provided by the CIT Division of Customer Support (DCS). It is a component of the Remedy Action Request System (ARS), the software product that DCS uses to perform this function.

The bidirectional connection between NED and the ARS customer database:

- Joins previously-created customer records to NED entries, thus associating HHS ID numbers with customer records and initializing locator information missing in NED. This is necessary because DCS must occasionally create service requests for individuals prior to their EoD date; that is, before their NED entry and HHS ID number have been activated.
- Creates customer records for all individuals.
- Updates name, locator, and organizational information in the customer database.
- Deactivates customer records when individuals separate from NIH.

## **NED OVERVIEW**

The customer database resides in a Oracle database. NED writes to the database via the proprietary ARS API and client library, and reads from it via ODBC.

The road to success is always under construction.

Arnold Palmer

## FUTURE WORK

### Improve Deregistration

NED has greatly improved, but not solved, the problem of reliably deregistering individuals when they separate from NIH. Thus, NED's largest data quality problem is the thousands of incorrectly active records for people, primarily Contractors, who are no longer affiliated with NIH, but have not been deregistered. Fundamentally, NIH has no timely business process for NED to hook into that is reliably performed when unpaid/non-visiting workers leave.

### Manage Organization and Buildings Data

NIH organization and buildings data has some of the same problems as its people data, though on a smaller scale:

- No database contains records for all organizations or buildings.
- No database contains all desired data elements.
- Organization/building names and abbreviations differ across databases.
- Data is not updated soon enough for use in NED.
- Data quality is lacking: missing/invalid values, inconsistently coded values, old data.

## Index

- accounts, 8, 10, 35
- Action Request System, 28, 36, 37
- Active Directory, 8, 18, 19, 23, 27, 28, 35, 36
- AD/NED Link Editor, 26, 27
- address book, 35
- Administrative Officers, 12, 15, 16, 17, 24, 27, 28, 34, 35, 36
- Administrative Technicians, 15, 16, 24, 26
- AMG Technical Subcommittee, 11, 12, 13, 14, 18
- Andover Controls, 17, 34
- application programming interface, 19, 37
- Architectural Management Group, 10, 11, 12, 13, 14, 18
- arrears, operation in, 14
- audit trail, 12
- authentication, 18, 35
- barcode, 34, 36
- building, 14, 23, 34, 38
- buildings, 9, 38
- Center for Information Technology, i, 15, 16, 18, 36
- Common Internet File System, 29, 30
- Connect
  - Direct, 30
- connector, 15, 16, 18, 19, 28, 29, 30
- content management, 17, 34
- Continuum, 17, 29, 34
- Contractor, 8, 35
- Control Data Systems, 14
- Conveyant TeleDirectory, 30, 35
- Critical Path, 15, 17, 18, 19, 26, 27
- date of birth, 8, 23
- DB2, 18, 19, 20, 28, 30
- delivery address, 8
- Department of Health and Human Services, 8
- deregistration, 8, 10
- Directory Information Tree, 12
- directory server, 12, 15, 17, 18, 19
- Directory Steering Committee, 15, 16, 18
- Division of Customer Support, 36
- Division of International Services, 28
- Division of Personnel Security and Access Control, 17, 28, 34
- Division of Public Safety, 17
- domain, 35, 36
- eDirectory, 15
- email, 8, 10, 18, 23, 35
- email address, 8, 23
- Email Directory and Forwarding Service, 16, 17, 18
- Employee, 8, 35
- Entrance on Duty date, 14, 37
- Exchange email, 35
- Fellowship Payment System, 18
- Guest, 8
- HELPCoconnect, 28
- HHS ID number, 8, 12, 13, 16, 24, 34, 36
- Human Resources Database, 8, 18, 28
- Hypertext Transfer Protocol, 25, 27
- IBM, 28, 30
- ID badge, 8, 14, 17, 34, 35
- ID badge title, 34
- ID photo, 8, 23, 34
- identity information, 8, 14, 23, 24, 34
- Information Technology Central Committee, 10, 11
- Innovative Interfaces, 36
- Institutes and Centers, 9, 10, 11, 15, 16, 17, 34, 35
- Integrated Time and Attendance System, 8, 16, 19, 20, 23, 29, 35, 36
- Internet Information Services, 25, 27
- ISOCOR, 14, 15
- J. E. Fogarty Database, 18, 20
- Join Engine, 12, 13, 14, 15, 16, 17, 18, 19, 24, 26, 27, 28, 29, 30, 34
- Library Patron Database, 18, 23, 34, 36
- Lightweight Directory Access Protocol, 11, 12, 15, 17, 26, 27, 28, 35
- locator information, 8, 14, 17, 23, 24, 36
- magnetic stripe, 34
- mailstop code, 26, 28
- Management Center, 27
- meta-directory, 12, 13, 14, 15, 16, 17, 18, 19, 24
- Microsoft, 15, 25, 27, 28, 29, 31, 32, 35
- National Cancer Institute, 9
- National Heart, Lung, and Blood Institute, 16
- National Institute of Environmental Health Sciences, 9, 17
- NED CAP, 20
- NEDWeb, 12, 15, 16, 17, 18, 19, 26, 27, 34, 35, 36
- Netegrity, 18
- Netscape, 14, 15
- NIH Almanac, 9

## NED OVERVIEW

NIH Business and Research Support System, 8, 18, 19  
NIH ID Badge Physical Access Control System, 17, 23, 29, 34  
NIH ID number, 12, 13, 17, 18, 23  
NIH Library, 29, 36  
NIH Login, 8, 18, 19, 23, 27, 35, 36  
Novell, 15  
Nsure Identity Manager, 15  
Office of the Director, 8  
ONEIDConnect, 29  
Open Directory, 14  
OPERConnect, 30  
Oracle, 16, 19, 26, 27, 28, 30, 31  
Oracle Data Customers, 30  
Oracle Transparent Gateway, 28  
organizational affiliation, 8  
organizational status, 34, 35  
organizational unit, 9  
OS/390, 18, 19  
parking, 10  
Parking and ID Badge System, 16  
Parking and Transhare System, 34  
Perl, 15, 19, 28, 29, 30  
Personal Identification Number, 12  
Personnel Data Import, 29  
place of birth, 8, 13, 23  
Privacy Act, 13, 15, 16, 23  
record linking, 16, 18  
registration, 8  
relational database, 8, 11, 16  
room number, 34  
schema, 12, 17  
Service Desk, 23, 27, 28, 30, 35, 36  
Service Desk Customer Database, 36  
SiteMinder, 18  
Social Security Number, 8, 11, 13, 14, 36  
SQL Server, 28, 29  
SQL\*Net, 26, 27, 30  
Structured Query Language, 11, 12, 26, 27, 28, 29, 30, 31  
Sun Microsystems, 15  
Teamworks, 25, 26, 28  
Telephone Directory, 16, 18, 23, 35  
telephone number, 8, 23, 34  
Telephone Operator Services, 35  
The Burton Group, 11, 14  
TIBCO, 30  
Visiting Fellows, 20  
Web Sponsor, 23  
Zoomit, 14, 15