NIH External Directory Domain Team Final Report

February 4, 2007
Version 1.1

Table of Contents

1.0 Domain Team Approach 3
1.1 Background 3
1.1.1 External Directory Domain Team 3
1.2 Approach 4
1.2.1 Scope 4
1.2.2 Alignment with the NIH Enterprise Architecture Framework 4
1.2.3 Analysis 5
1.2.4 Recommendation 5
2.0 Analysis 6
2.1 Introduction 6
2.2 External Active Directory Technical Solution 6
2.3 Intended Uses 7
2.4 Business Process Models 8
2.4.1 Setup/Modify External Directory Project 10
2.4.2 Setup Registration Authority Relationship 11
2.4.3 Update Group Membership 12
2.4.4 Conduct Level 2 Identity Proofing: In-Person 13
2.4.5 Conduct Level 2 Identity Proofing: Remote 14
2.4.6 Update Account Profile 15
2.4.7 Decommission Account via Request 16
2.4.8 Decommission Account via Inactivity 17
2.4.9 Close External Directory Project 18
2.5 Data Requirements 18
3.0 Recommendation 21
3.1 Introduction 21
3.2 Overall Recommendation 21
3.3 Gap Analysis 21
Appendix I: Process Models 22
Setup/Modify External Directory Project 22
Setup Registration Authority Relationship 23
Update Group Membership 24
Conduct Level 2 Identity Proofing: In-Person 25
Conduct Level 2 Identity Proofing: Remote 26
Update Account Profile 27
Decommission Account via Request 28
Decommission Account via Inactivity 29
Close External Directory Project 30
Appendix II: Glossary of Terms 31
Appendix III: References 32
Change History 33

1.0 Domain Team Approach

1.1 Background

The Office of the Chief IT Architect (OCITA) commissions domain teams to develop enterprise architecture artifacts within a specific National Institutes of Health (NIH) Enterprise Architecture (EA) domain. The domain team products generated by this process are developed by documenting the research, analysis and recommendations reached through consensus in the domain team meetings.

The Technology Transformation Plan[5] segment of OCITA's Program Plan focuses on implementing various technologies that enable NIH to transition from the "as-is" to the planned "to-be" architecture. One such proposal in the plan is Coordinate Identity Management Initiatives. OCITA has a long range vision to register both people within the NIH and outside the NIH to grant them access to appropriate systems.

In addition, several business owners expressed an immediate need for external users to access NIH systems. In the near term, the NIH External Active Directory (AD) solution addresses the business owners' needs as well as providing a path forward in meeting OCITA's long range vision.

Federal systems are subject to a variety of Federal regulations. In particular, the Office of Management and Budget (OMB) has issued guidance to Federal agencies to ensure that online government services are secure and protect user's privacy[1]. To accomplish this guideline, some type of identity verification or authentication is needed. As such, OMB directs agencies to conduct E-Authentication risk assessments on electronic transactions to ensure that authentication processes provide the appropriate levels of assurance. E-Authentication is the process of establishing confidence in a user's identity which is presented electronically. The four levels of identity assurance are defined as follows:

- **Level 1:** Little or no confidence in the asserted identity's validity
- **Level 2:** Some confidence in the asserted identity's validity
- **Level 3:** High confidence in the asserted identity's validity
- **Level 4:** Very high confidence in the asserted identity's validity

Building upon these regulations, OCITA commissioned an External Directory Domain Team, comprised of professionals throughout the NIH's various Institutes and Centers (ICs), to document the standards and requirements for user registration, management, and deregistration from the NIH Active Directory (AD) external directory – NIH External.

1.1.1 External Directory Domain Team

The External Directory Domain Team, a team of individuals from various NIH ICs, worked together for six weeks to develop the proposed process models and data requirements contained in this report. The team consisted of individuals representing a variety of areas, including technologists, scientists, users, security, and policy. The following table identifies the domain team members who contributed to this effort and the ICs they represent.

External Directory Domain Team: Participants			
Name	**Affiliation**	**Name**	**Affiliation**
Peter Alterman	CIT	Vikas Khator	CIT
Ben Rassuli	NIDCR	Todd Myrick	CC
Bill Barrick	NIAID	Ric Rodriguez	OD
Debbie Bucci	CIT	Helen Schmitz	OCITA
Lee Butler	NHLBI	Mark Silverman	OCITA

External Directory Domain Team: Participants			
Name	**Affiliation**	**Name**	**Affiliation**
Janet David	NIAMS	Steve Thornton	OCITA
Ron Davis	NCRR	Linda Tomlinson	NIGMS
Jim Dix	NIEHS	Jim Tucker	OD
Jeff Erickson	CIT	Valerie Wampler	CIT
Judy Fabrikant	CIT	Adrienne Yang	CIT
Al Graeff	NLM		

1.2 Approach

1.2.1 Scope

The External Directory Domain Team was chartered to review the NIH External processes already in place, build upon them and document the resulting process models. The primary purpose of the domain team was to address NIH business needs around external user authentication and authorization while ensuring the appropriate controls are instantiated to protect the NIH environment and data. The processes for managing users in Commons were not addressed at this time.

To accomplish this goal, the group concentrated on the following objectives:

- Understand the current AD External Directory solution at NIH, including the processes which currently support it
- Investigate potential uses for the AD External Directory to determine the appropriate level of authentication assurance levels required
- Determine the processes for managing the external directory from account request through account close
- Ensure the defined processes comply with Federal regulations[1, 4]
- Define supporting data requirements
- Identify recommendations and next steps

1.2.2 Alignment with the NIH Enterprise Architecture Framework

The NIH EA Framework, as depicted in the figure below, consists of three distinct architectures: business architecture, information architecture, and technical architecture. The External Directory Domain Team's work was focused in the Business Architecture as well as the Data Domain of the NIH Information Architecture.

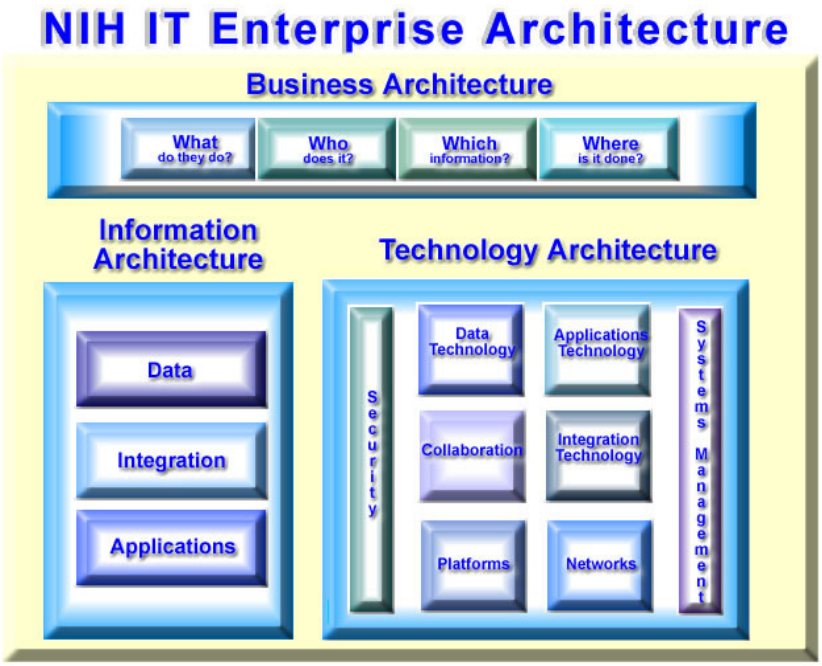


Figure 1: NIH EA Framework

To learn more about the NIH EA framework, visit the NIH EA Website[2].

1.2.3 Analysis

The domain team focused its analysis on developing the process models for administering NIH External. To reach their objectives and develop these recommendations, the group employed a variety of techniques. These methods include:

- A review of applicable Federal regulations regarding E-Authentication, including, but not limited to:
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63: Electronic Authentication Guideline
  - Office of Management and Budget (OMB) M-04-04: E-Authentication Guidance for Federal Agencies
- An assessment of the intended uses for the External Directory as well as potential projects and their corresponding risk assessment levels. This assessment was used to determine the E-Authentication levels that the External Directory solution and processes must support.
- An assessment of the existing processes in place for the Active Directory External Directory at NIH. These processes were used as the foundation for the models developed by the domain team, as well as the supporting data requirements.

The findings from the above research and analysis are documented in the Analysis section of this report.

1.2.4 Recommendation

The domain team's findings from the research were then analyzed to draft recommendations and next steps regarding the External Directory at NIH and are described in the Recommendation section of this report.

2.0 Analysis

2.1 Introduction

The following section details the results from research conducted by the domain team and the associated process models from the analysis of the research materials. This information was used to develop the domain team's recommendations and next steps regarding the External Directory.

2.2 External Active Directory Technical Solution

NIH External (nihext.nih.gov), the Active Directory (AD) External Directory solution at NIH, is a Microsoft Windows 2003 Active Directory Forest. Its purpose is to provide authentication and authorization to non-NIH affiliated staff requiring access to NIH applications and data. The Active Directory forest implemented at NIH is depicted in the image below. There is a one-way trust between nih.gov and nihext.nih.gov. NIH External acts as a Credential Service Provider (CSP).

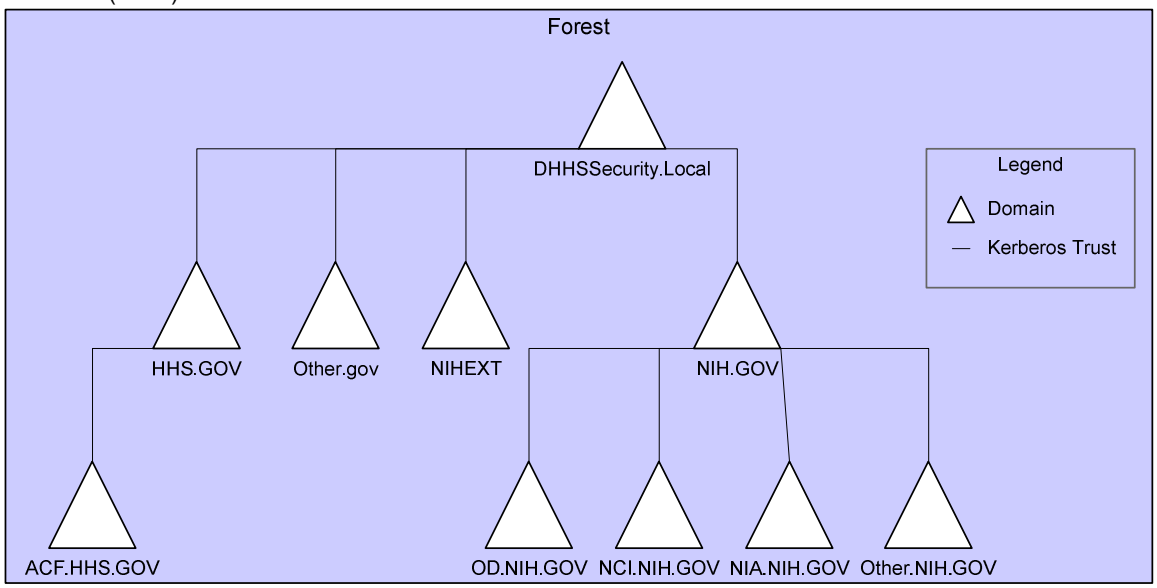


Figure 2: NIH External Active Directory Forest

Unlike the internal Active Directory structure, NIH External's structure is project-based, allowing for cross-project membership. An organizational unit (OU) is the smallest scope item to which group policies/rights can be assigned. Organizational units can be used to create containers within a domain, in this case NIH External, which represent the hierarchical, logical structures within an organization. This project-based, NIH External OU structure is captured in the image below.

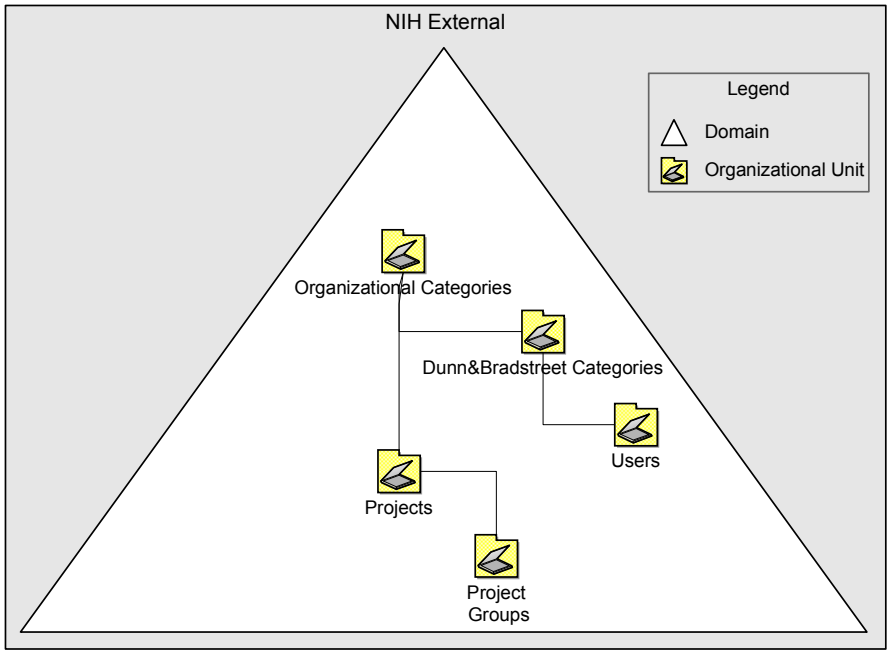


Figure 3: NIH External Active Directory Structure

NIH External follows AD data content management standards. (See the Data Requirements section of this report.) In addition, NIH External follows nih.gov password complexity and expiration policies[3]. However, the Center for Information Technology (CIT) is currently working with the Incident Response Team (IRT) to amend the current policy in order to require a shorter, 90-day password expiration term for NIH external. Finally, because NIH External is intended for authentication and authorization only, NIH External accounts will not have email or Virtual Private Network (VPN) access.

2.3 Intended Uses

When implementing services electronically, Federal agencies must determine the level of assurance necessary for authenticating transactions. Some of the basic technical requirements for each assurance levels are[4]:

- **Level 1:** There is no identity proofing requirement at this level. Successful authentication requires that a claimant prove through a secure mechanism protocol they he or she controls the token. For example, a password token - a secret that a claimant memorizes and uses to authenticate his or her - identity may be used.
- **Level 2:** Identity proofing of individuals is required. Successful authentication requires the claimant prove that he or she controls the token. The system must provide single factor remote authentication.
- **Level 3:** Identity proofing of individuals is required. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, must use a password in a secure authentication protocol. Multi-factor authentication is introduced at this level.
- **Level 4:** Identity proofing is required. Successful authentication is based of proof of possession of a key through a cryptographic protocol. This level is similar to level 3 with the exception that only “hard” tokens are accepted. A “hard” token is a hardware device that contains a protected cryptographic key.

NIH External is capable of authenticating users at levels 1 and 2. The processes involved for a level 2 system are more complex than those for level 1. Given the complexity, specifically around the processes for identity proofing individuals, it was important to determine whether

a need for a Level 2 system was required at NIH prior to focusing the domain team's effort on Level 2.

The following potential uses were identified by the External Directory Domain team as the types of activities might require external user access:

- Collaboration
- Document management and sharing
- Extramural programs
- Participation in studies

The domain team identified the following applications that might require external user access:

- Microsoft SharePoint sites
- NIH Portal
- Adobe Macromedia Breeze
- NIH wiki
- Genetic Association Information Network (GAIN)
- Information for Management, Planning, Analysis, and Coordination (IMPAC) II
- Server Message Block (SMB) servers
- Open Text LiveLink

The potential uses and applications lists above are by no means exhaustive; however, it is apparent from this list that an authentication system put in place at NIH to handle external users must provide both Levels 1 and 2 E-Authentication.

2.4 Business Process Models

All work in an organization gets done through activities performed for a purpose. A business process is a sequence of activities performed according to certain business rules. Each activity is performed by a person (or system) at place and time using certain information. The benefits of modeling business processes include:

- Shared understanding of processes
- Repeatable and standardized processes
- Efficient and productive organizations
- Basis for planning and future process improvements
- Ensuring compliance with necessary regulations

Business process modeling seeks to answer the following questions:

- What activities must the business perform to achieve its purpose?
- Which information is used to perform each activity?
- Who performs each activity?
- When are the activities performed?
- Where are the activities performed?

The business process models below seek to answer these questions in a comprehensive model that captures the sequence of activities, and the flow of information – which and who – from one activity to another.

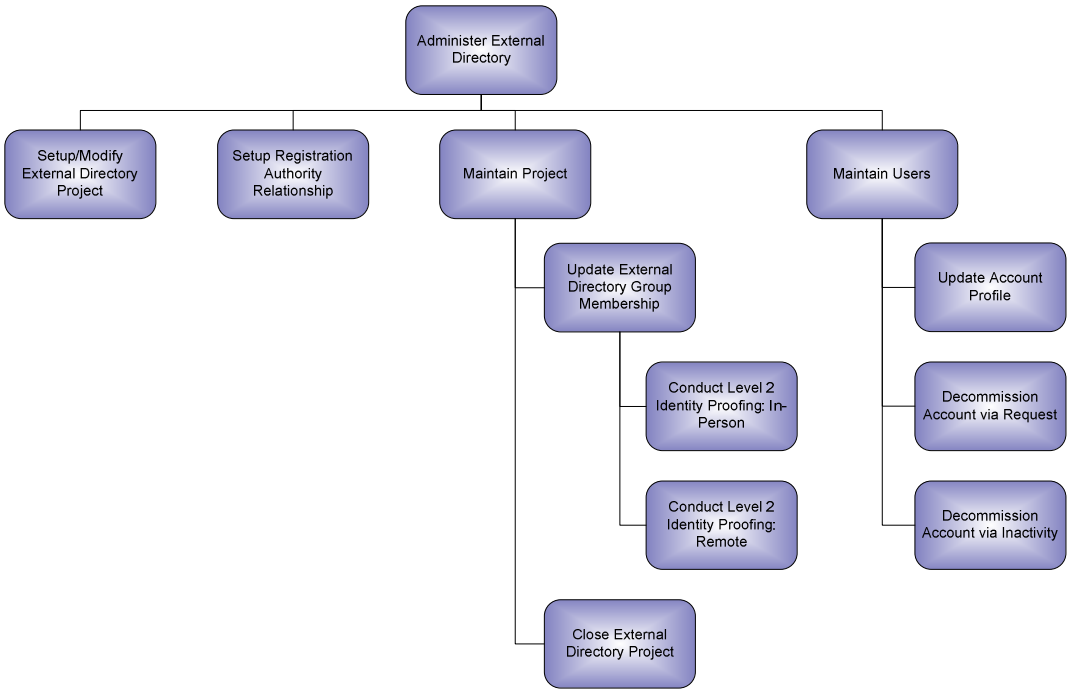
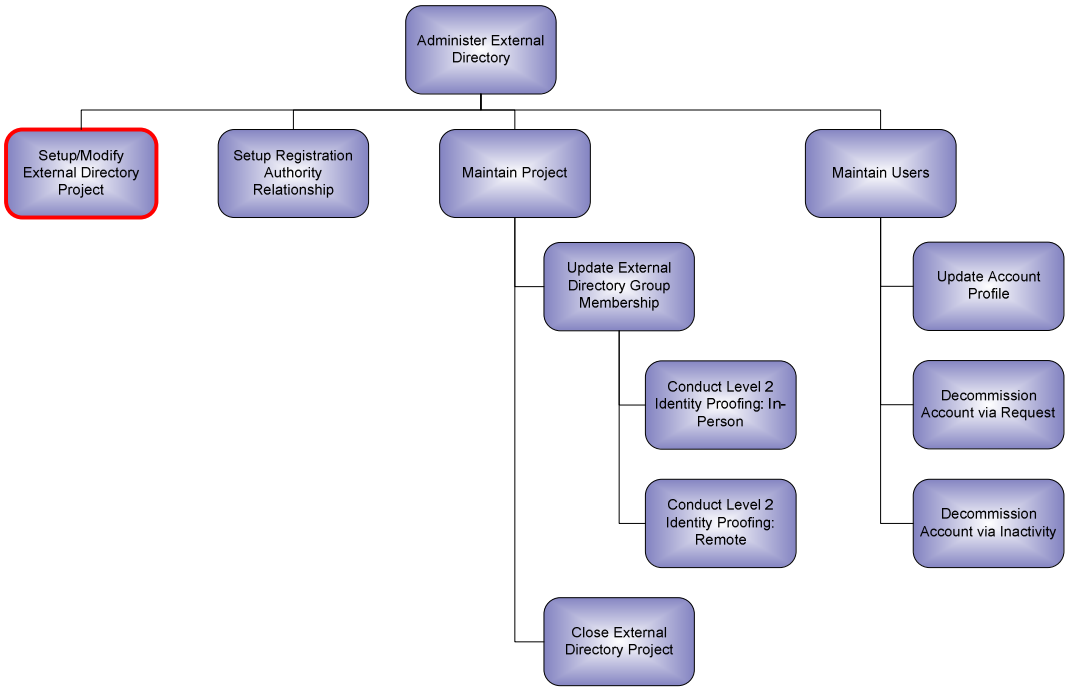


Figure 4: NIH External Directory Process Models

The External Directory Process Models, depicted in the image above, incorporate the activities necessary to administer NIH External, the Active Directory external directory solution at NIH.

Specific details regarding each model are described in the following sections. Any assumptions made in developing the model are clearly defined. In such cases as gaps or recommendations were identified, they are collated in the Recommendation section of this report. As determined during the analysis of intended uses, the models and activities described below for this system support level 1 and 2 E-Authentication.

2.4.1 Setup/Modify External Directory Project



The Setup/Modify External Directory (ED) Project model describes the series of activities necessary for an ED project sponsor to have an ED project setup in NIH External for the purposes of authenticating and authorizing external users. External Directory projects will need to be renewed every year. This will help reduce the proliferation of inactive projects within NIH External. CIT is responsible for notifying ED project sponsors regarding renewing their Service Level Agreement. With the exception of the administrators group in nih.gov, called out as Admin Group in step 1.6 in the process model, all ED project groups are created in NIH External. Administrators added to ED project groups manage project group membership throughout the project lifecycle. The ED project sponsor should be responsible for completing the risk assessment and notifying the IC Information System Security Officer (ISSO).

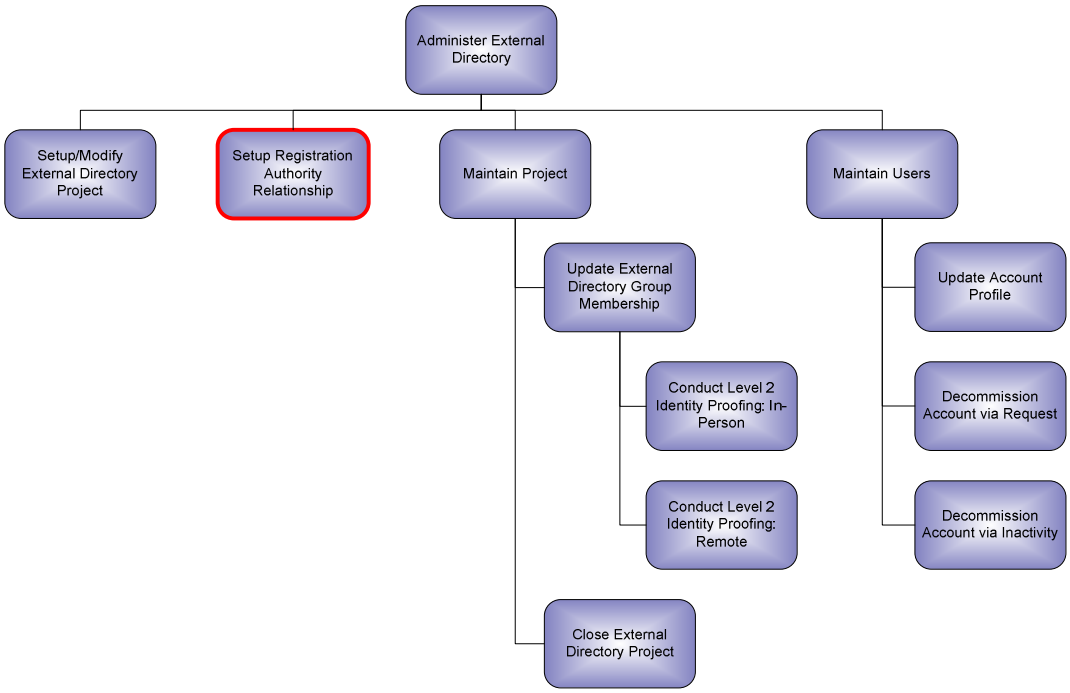
Refer to Appendix I Process Models: Setup/Modify External Directory Project in order to view the model.

2.4.1.1 Assumptions

The following assumptions were made during the definition of this process:

- Project Sponsor has determined that external user access is necessary.
- Risk assessment to determine E-Authentication level for the ED project is complete.
- ED Project group names must follow the standard defined in NRFC0007, Group Naming Standard.

2.4.2 Setup Registration Authority Relationship



Federal regulations[1, 4] stipulate systems with an E-Authentication level of 2 or above must provide some assurance that users are who they say they are. This involves identity proofing external users prior to registration within NIH External. A Registration Authority is the individual responsible for accomplishing this task.

Registration Authorities act on behalf of the NIH, but do not need to be NIH employees. The Setup Registration Authority Relationship model describes the activities required to establish a relationship with an RA.

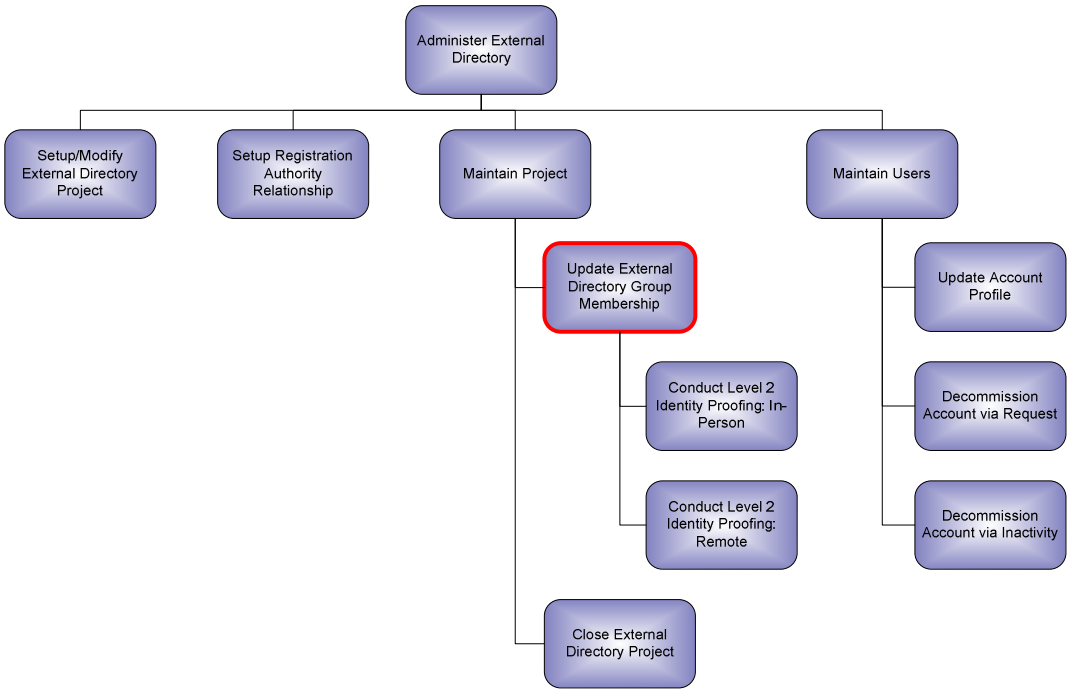
Please refer to Appendix I Process Models: Setup Relationship with Registration Authority in order to view the model.

2.4.2.1 Assumptions

The following assumptions were made during the definition of this process:

- Central database of Registration Authorities acting on behalf of NIH exists and is available to ED Project Sponsors. (See the Recommendation section of this report.)
- Agreement with the Registration Authority includes language that the RA will conduct the correct identity proofing process.

2.4.3 Update Group Membership



Throughout an ED project's lifecycle within NIH External, it is necessary to update the membership of its project groups. The Update Group Membership model describes the activities involved in adding, removing, and moving external users within an ED project. As the external directory supports both levels 1 and 2 E-Authentication, this model accounts for proper identity proofing procedures. When identity proofing is required, the Level 2 Identity Proofing: In-Person and Level 2 Identity Proofing: Remote process models are used.

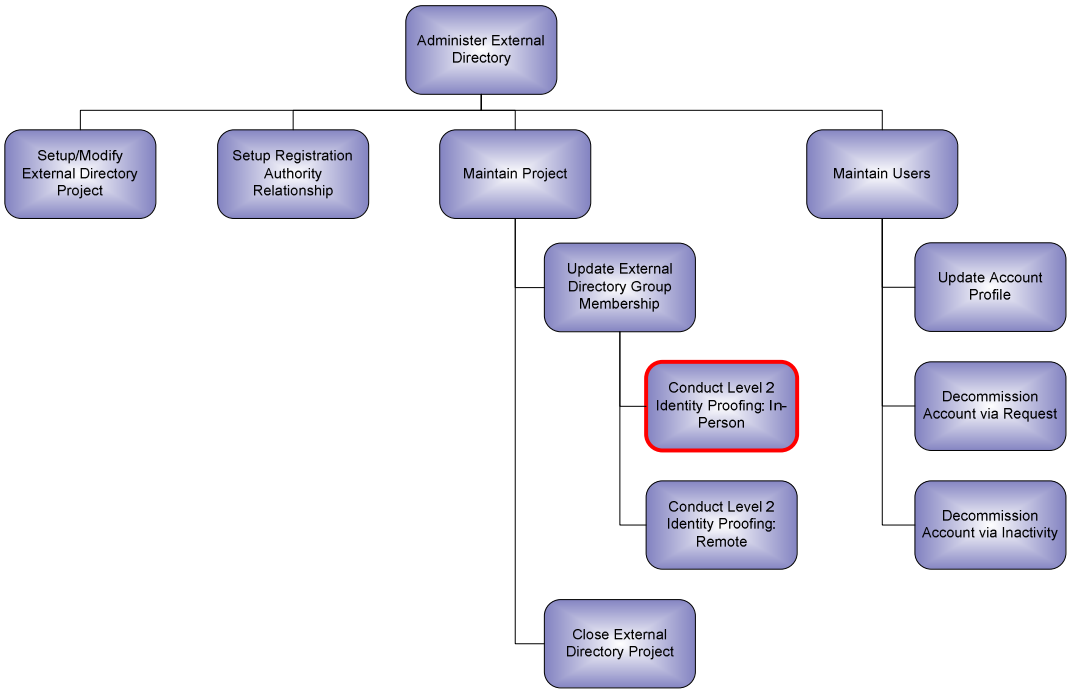
Refer to Appendix I Process Models: Update Group Membership in order to view the model.

2.4.3.1 Assumptions

The following assumptions were made during the definition of this process:

- ED Project Identifier is persistent, even if ED project is removed from NIH External.
- ED Projects requiring an E-Authentication level of 2 have a relationship with a Registration Authority (RA) to perform identity proofing of candidate external users.

2.4.4 Conduct Level 2 Identity Proofing: In-Person



The registration and identity proofing process is designed to ensure that the Registration Authority confirms the identity of the applicant. When an applicant is able to appear in person to the Registration Authority, the Conduct Level 2 Identity Proofing: In-Person process is followed.

Refer to Appendix I Process Models: Conduct Level 2 Identity Proofing: In-Person in order to view the model.

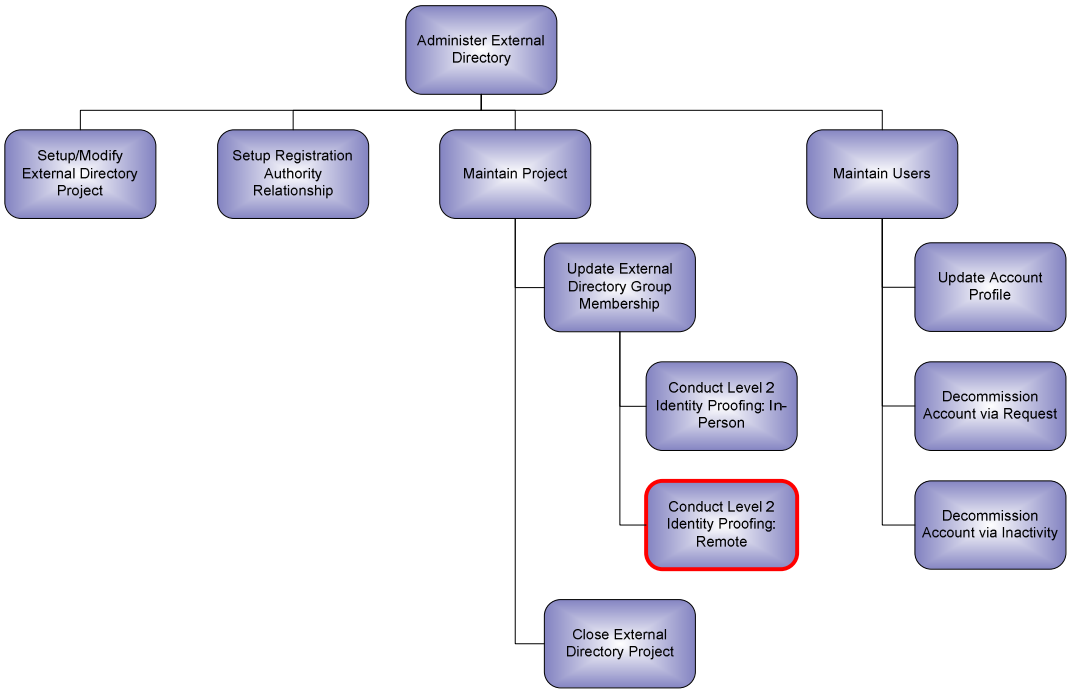
To participate in this process, an applicant must possess a valid, non-expired government photo ID. Examples of such IDs include a driver's license or passport. Given the number of different countries in which active collaboration occurs with the NIH, the External Directory Domain Team concludes that non-U.S. government photo IDs must be accepted by an RA as well. Step 2.2, Inspect ID, involves two steps: comparing the picture on the ID to the applicant and determining if the ID appears to be valid. In the model, address of record is defined as that provided by the applicant in their application.

2.4.4.1 Assumptions

The following assumptions were made during the definition of this process:

- RA is acting on NIH's behalf, and if external to NIH, has participated in the Setup Registration Authority Relationship process.
- A system for recording the information collected from the applicant exists. (See Recommendation section of this report.)
- Recording the information for applicants who do not pass identity proofing is not necessary.

2.4.5 Conduct Level 2 Identity Proofing: Remote



When an applicant is not able to appear in person to the Registration Authority, the Level 2 Identity Proofing: Remote process is followed to identity proof the applicant.

Refer to Appendix I Process Models: Conduct Level 2 Identity Proofing: Remote in order to view the model.

The Personally Identifiable Information (PII) provided by the applicant must include their name, address, and telephone number. Given the number of different countries in which active collaboration occurs with the NIH, the External Directory Domain Team concludes that additional PII provided by the applicant may include the following:

- Government ID number
- Financial account number
- Social Security Number
- Visa number
- Green card number
- Reputable organization name of which applicant is a member

Secure website, fax, postal mail, email and phone are all acceptable methods for supplying PII to the Registration Authority. Due to the wide variety of PII that may be provided by an applicant, the method of conducting a record check may vary. Examples methods include:

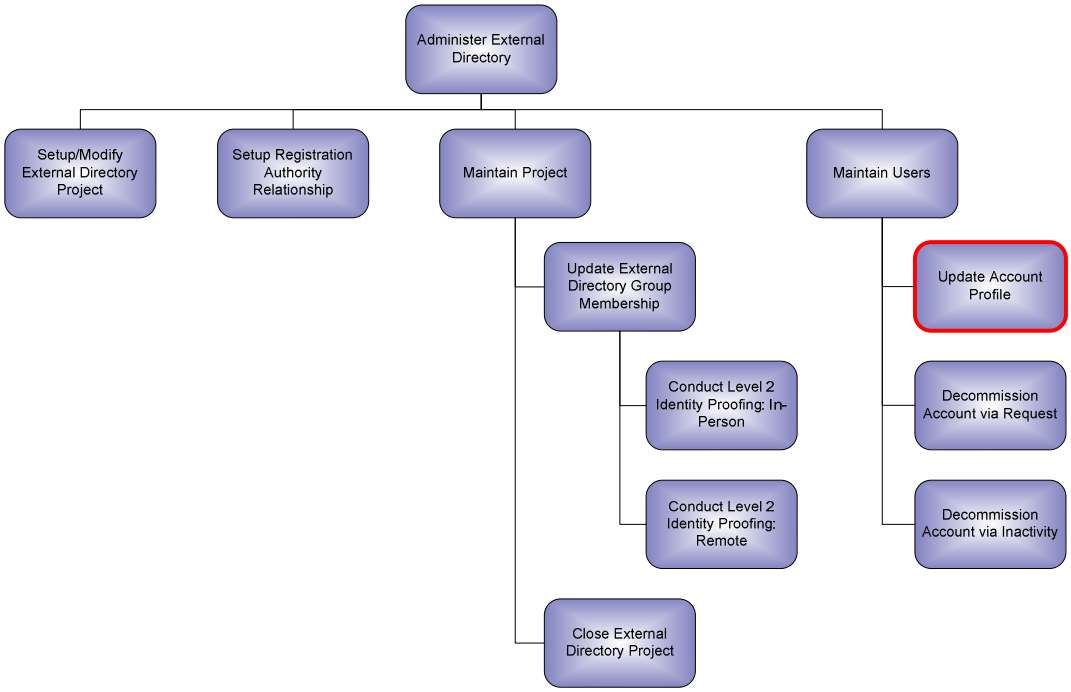
- Contacting the reputable organization and verifying PII recorded with that provided by applicant
- Contacting issuing organization of ID and verifying information
- Conducting a credit check with a company such as Equifax

2.4.5.1 Assumptions

The following assumptions were made during the definition of this process:

- RA is acting on NIH's behalf, and if external to NIH, has participated in the Setup Registration Authority Relationship process.
- A system in which to record the information collected in this process exists. (See the Recommendation section of this report.)
- Recording the information for applicants who do not pass identity proofing is not necessary.

2.4.6 Update Account Profile



During the lifetime of an external user account within NIH External, it may become necessary for the user to update their personal information. The Update Account Profile model describes the steps necessary for a user to do so.

Refer to Appendix I Process Models: Update Account Profile in order to view the model.

To update their identifying information, an NIH External user must contact the NIH Help Desk. (See the Recommendation section of this report for alternate methods to accomplish this process in the future.)

The attributes a user may update include:

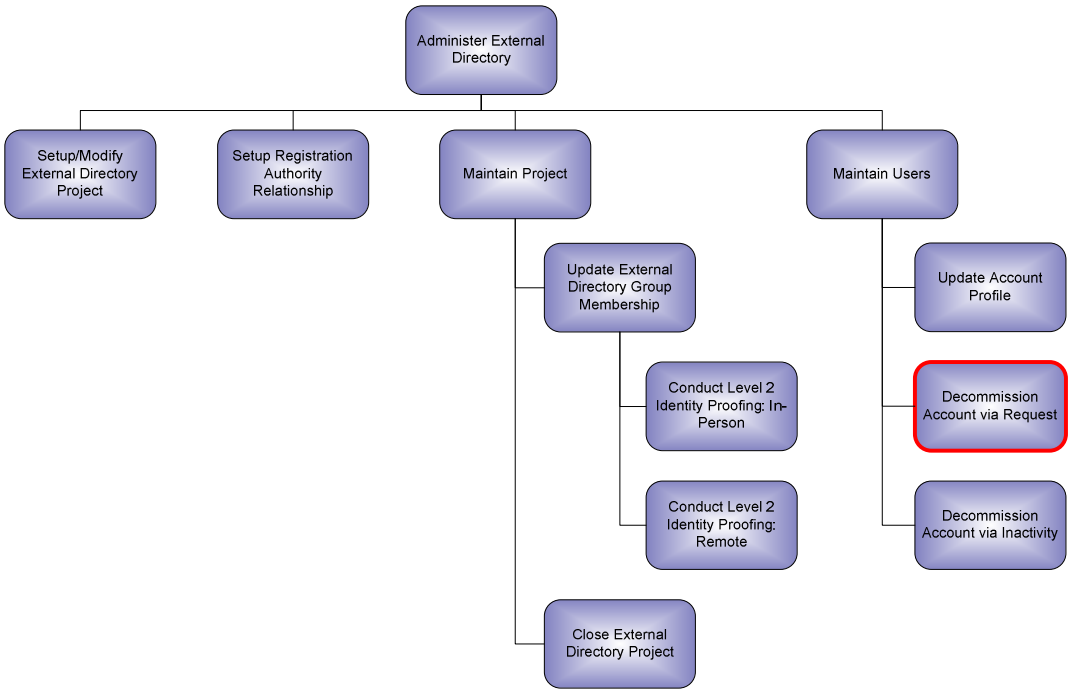
- Company
- Department
- Email address
- Street address
- City
- State
- Country
- Postal code
- Telephone number

2.4.6.1 Assumptions

The following assumptions were made during the definition of this process:

- The user is already authenticated.

2.4.7 Decommission Account via Request



The Decommission Account via Request model illustrates the process through which an NIH External account can be decommissioned. Two events may kick-off this process: external user requests an account be closed; suspected NIH External account abuse occurs. Disabled accounts that remain inactive will be decommissioned through the Decommission Account via Inactivity process.

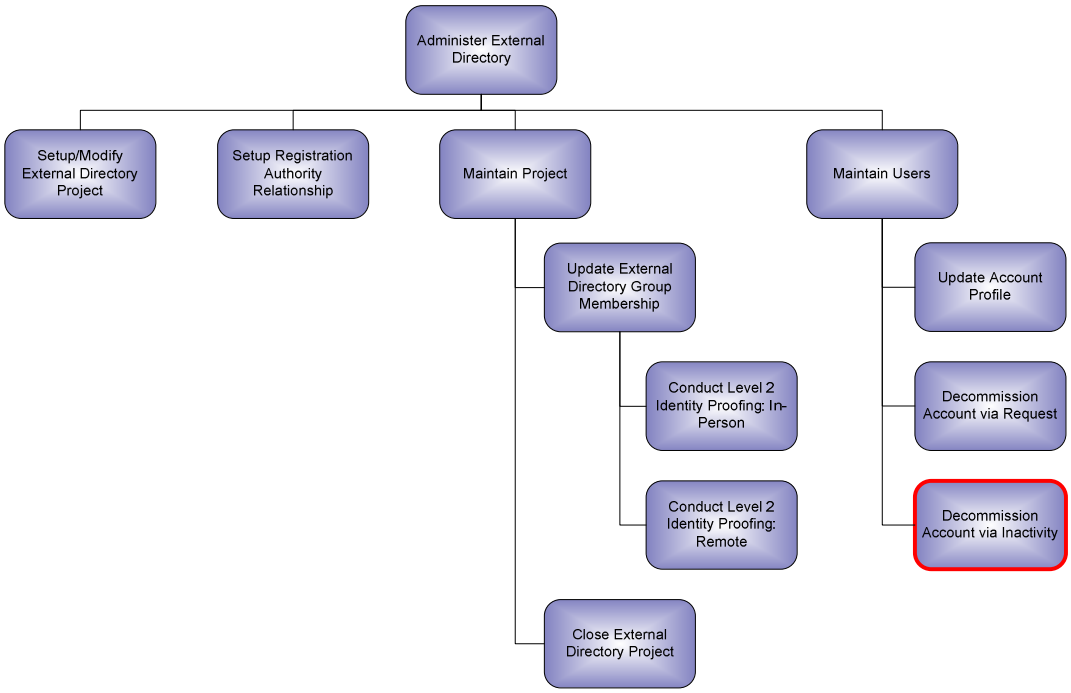
Refer to Appendix I Process Models: Decommission Account via Request in order to view the model.

2.4.7.1 Assumptions

The following assumptions were made during the definition of this process:

- An external user may request their account be decommissioned through Email or through the NIH Help Desk.

2.4.8 Decommission Account via Inactivity



One of the underlying issues in the current internal Active Directory solution is the prevalence of accounts which are inactive. To address this problem, the Decommission Account via Inactivity process model is presented below. NIH External accounts must belong to at least one ED project and the account password must be updated at least every 90-days. This clean-up process provides a mechanism for removing orphaned accounts, as well as those accounts that have been inactive for a period of time.

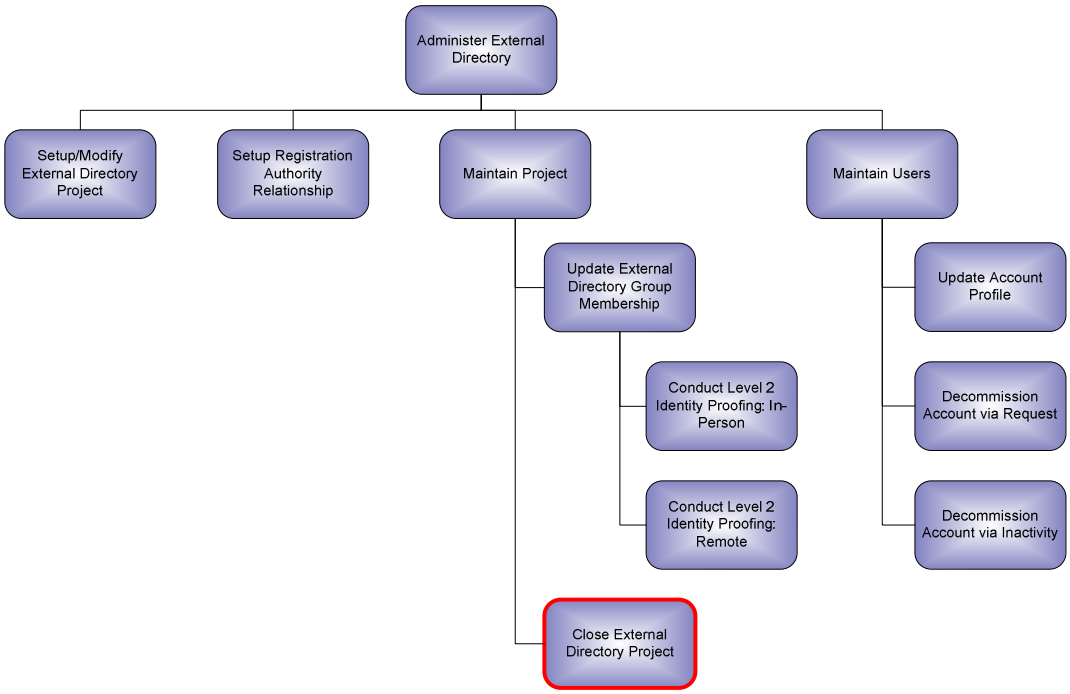
Please refer to Appendix I Process Models: Decommission Account via Inactivity in order to view the model.

2.4.8.1 Assumptions

The following assumptions were made during the definition of this process:

- External user has been receiving password expiration notices according to the NIH External password expiration policy.
- External user has been able to update their password in accordance with the NIH External password expiration policy.

2.4.9 Close External Directory Project



The Close External Directory Project process model depicts the activities that must occur for an ED Project Sponsor to close an NIH External project. When a project is closed, it is a potential that users accounts may no longer be members of any project. One of the guiding principles of the NIH External architecture is that user accounts must belong to at least one group. As such, in the occurrence of such an event, orphaned accounts will be handled through the Decommission Account via Inactivity process.

Refer to Appendix I Process Models: Close External Directory Project in order to view the model.

2.5 Data Requirements

In the process models developed for NIH External, a wide range of data is collected in various activities. The artifacts involved in these processes include the ED Project Request, the External Directory Service Level Agreement and the External Directory Account Application. Information from these artifacts is stored in a variety of places, including Active Directory. In the future, additional applications may also store this data. As systems rely on these attributes, it is important to clarify what data is stored in the NIH External Active Directory.

The table below details the data attributes that are collected throughout the process models, the source of the data attribute, and the corresponding Active Directory attribute, where applicable.

ED Project Data				
Attribute	**Source**	**Valid Values**	**Active Directory Attribute**	**Example**
ED Project Name	ED Project Request	-	-	“GAIN”
ED Project Unique Identifier	ED Project Request	-	-	“GAIN23”
ED Project Sponsor Given Name	ED Project Request	-	-	“John”

ED Project Data				
Attribute	**Source**	**Valid Values**	**Active Directory Attribute**	**Example**
ED Project Sponsor Surname	ED Project Request	-	-	“Jones”
ED Project Sponsor NED ID	ED Project Request	-	-	123-4567-890
Backup ED Project Sponsor Given Name	ED Project Request	-	-	“John”
Backup ED Project Sponsor Surname	ED Project Request	-	-	“Jones”
Backup ED Project Sponsor NED ID	ED Project Request	-	-	123-4567-890
ISSO Given Name	ED Project Request	-	-	“John”
ISSO Surname	ED Project Request	-	-	“Jones”
ISSO NED ID	ED Project Request	-	-	123-4567-890
CIT Account Number	ED Project Request	-	-	“ABC1”
Agency Location Code	ED Project Request	-	-	75038928
ED Project Group	ED Project Request	-	projectGroup	“External Users”
ED Project Group E-Authentication Level	ED Project Request	1,2	groupEauthLevel	2
ED Project Term	ED Project Request	-	-	“18 months”
ED Project Administrator	ED Project Request	-	-	“John D. Smith”
ED Project E-Authentication Level	ED Project Request	1, 2	-	2
CIO Given Name	ED Project Request	-	-	“John”
CIO Surname	ED Project Request	-	-	“Jones”
Date of Agreement	External Directory Service Level Agreement	-	-	01/01/2006
Type of Agreement	External Directory Service Level Agreement	“New Agreement”, “Renewal Agreement”, “Modification to Current Year Agreement”	-	“New Agreeement”
Date Closed	External Directory Service Level Agreement		-	09/01/2006
CIO Sign-Off	External Directory Service Level Agreement	“Yes”, “No”	-	“Yes”
Agreement to E-Authentication Level	External Directory Service Level Agreement	“Yes”, “No”	-	“Yes”

External User Data				
Attribute	**Source**	**Valid Values**	**Active Directory Attribute**	**Example**
User Given Name	External Directory Application		givenName	“Mary-Lou”

External User Data				
Attribute	**Source**	**Valid Values**	**Active Directory Attribute**	**Example**
User Middle Name	External Directory Application		-	"Beth"
User Surname	External Directory Application		sn	"O'Connell"
Company	External Directory Application		company	"Harvard"
Street Address	External Directory Application		streetAddress	"12 Main St."
City	External Directory Application		l	"Bethesda"
State/Province	External Directory Application		st	"MD" "Quebec"
Country	External Directory Application		countryCode	"US"
Postal Code	External Directory Application		postalCode	"22152" "MK4 1B4"
Email Address	External Directory Application		mail	"smtp:smilthj@harvard.edu"
Telephone Number	External Directory Application		telephoneNumber	"55.1.4365.2374 x3709"
E-Authentication Level	External Directory Application		eAuthLevel	2
ED Project Name	External Directory Application		-	"GAIN"
ED Project Unique Identifier	External Directory Application		projectIdentifier	"GAIN23"
Application Status	External Directory Application		-	"Approved – Account Pending"

Registration Authority (RA) Data				
Attribute	**Source**	**Valid Values**	**Active Directory Attribute**	**Example**
RA Given Name	Registration Authority	-	-	"Mary-Lou"
RA Middle Name	Registration Authority	-	-	"Beth"
RA Surname	Registration Authority	-	-	"O'Connell"
Company	Registration Authority	-	-	"Harvard"
Street Address	Registration Authority	-	-	"12 Main St."
City	Registration Authority	-	-	"Bethesda"
State/Province	Registration Authority	-	-	"MD" "Quebec"
Country	Registration Authority	-	-	"US"
Postal Code	Registration Authority	-	-	"22152" "MK4 1B4"
Email Address	Registration Authority	-	-	"smtp:smilthj@harvard.edu"
Telephone Number	Registration Authority	-	-	"55.1.4365.2374 x3709"
E-Authentication Level	Registration Authority	1, 2	-	2

3.0 Recommendation

3.1 Introduction

Based on the analysis of the research findings, including the intended uses, technical solution and process models, the domain team's recommendation for the NIH External Directory is described in this section.

3.2 Overall Recommendation

The External Directory Domain Team formulated the following recommendations for NIH IT leadership to consider as it moves forward with the NIH External solution and process models contained in this report:

- Domain Team members should actively communicate the findings in this report to help educate the NIH community about NIH External and how the external directory can be used to their benefit.
- While the process described in this report can be accomplished in a manual fashion, a web application would decrease the arduousness of most of the processes. The Domain Team recommends that a web application system be built for NIH External.
    - A web application would reduce the burden on NIH staff to respond to applicant and user demands.
    - The Level 2 Identity Proofing: Remote process record check is conducted in a manual fashion. Commercial systems do exist in which a record check can be conducted against an identity. Most of these systems enable other application systems to communicate electronically with them, increasing the speed and ease in which this process can be completed.
- As NIH External has the capability to handle multiple E-Authentication levels, ED project risk assessments become critical to ensuring the security of NIH data and information. The creation of a standardized risk assessment for ED projects to follow would help ensure the appropriate categorization of ED projects.

3.3 Gap Analysis

The domain team identified the following as gaps that need to be considered as IT leadership moves forward in the implementation of the findings contained in this report:

- The Update Group Membership process model, as well as the Conduct Level 2 Identity Proofing models, identifies a need to store applicant data in a system outside of the Active Directory; Personally Identifiable Information (PII) cannot be stored in NIH External, as it is not accredited.
    - NED is one such suggested system, but a further analysis into requirements and implications is necessary prior to recommending a system of choice.

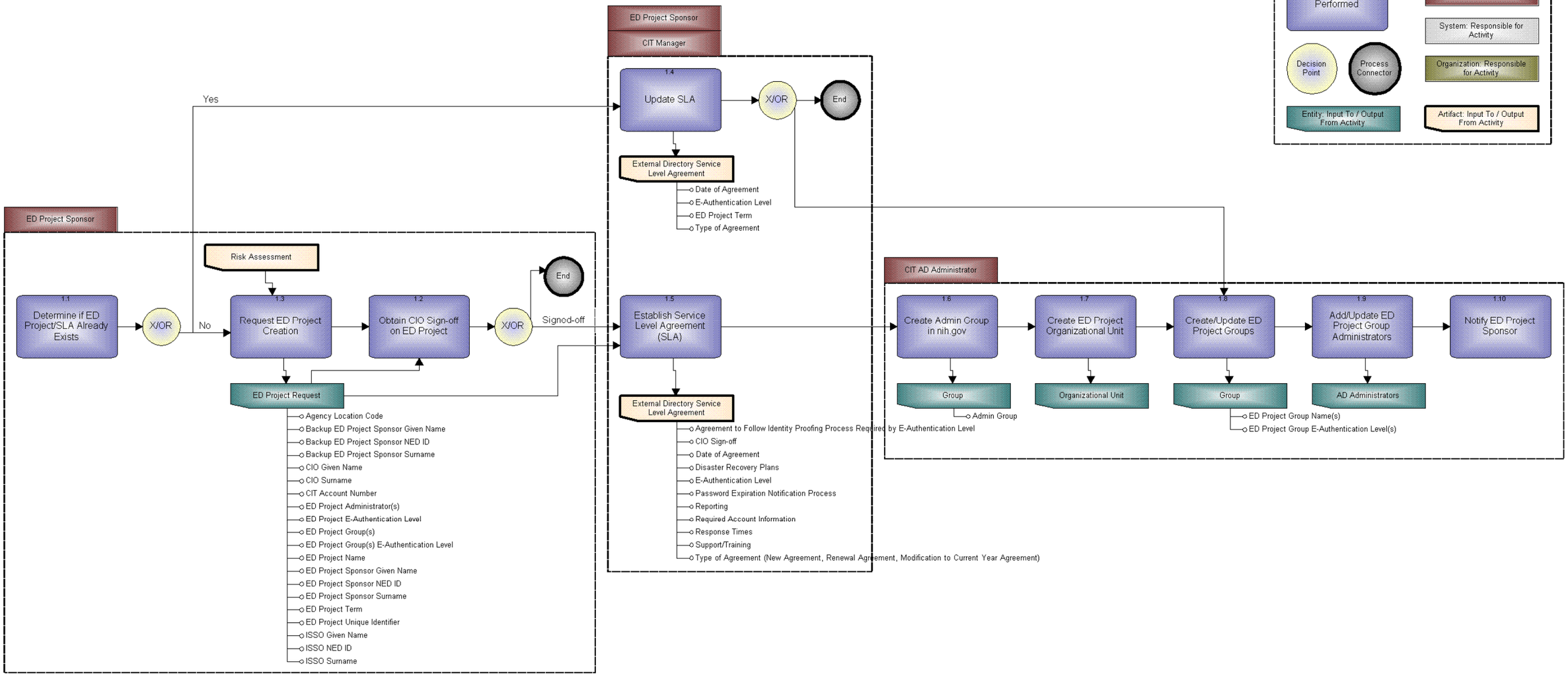
Appendix I: Process Models

Setup/Modify External Directory Project

External Directory

Setup/Modify ED Project Process Model

As-of: 2007.01.29



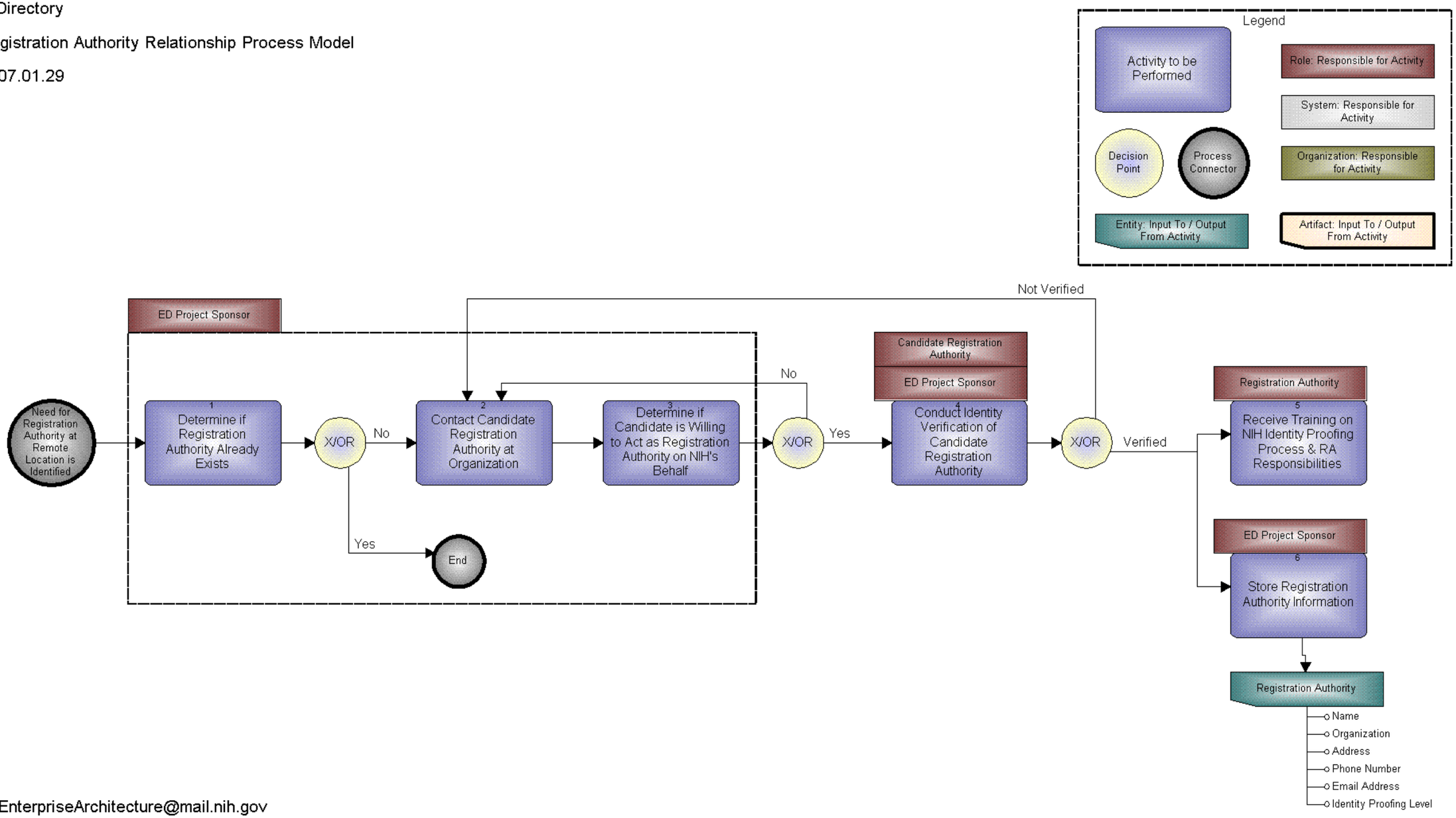
Contact: EnterpriseArchitecture@mail.nih.gov

Setup Registration Authority Relationship

External Directory

Setup Registration Authority Relationship Process Model

As-of: 2007.01.29



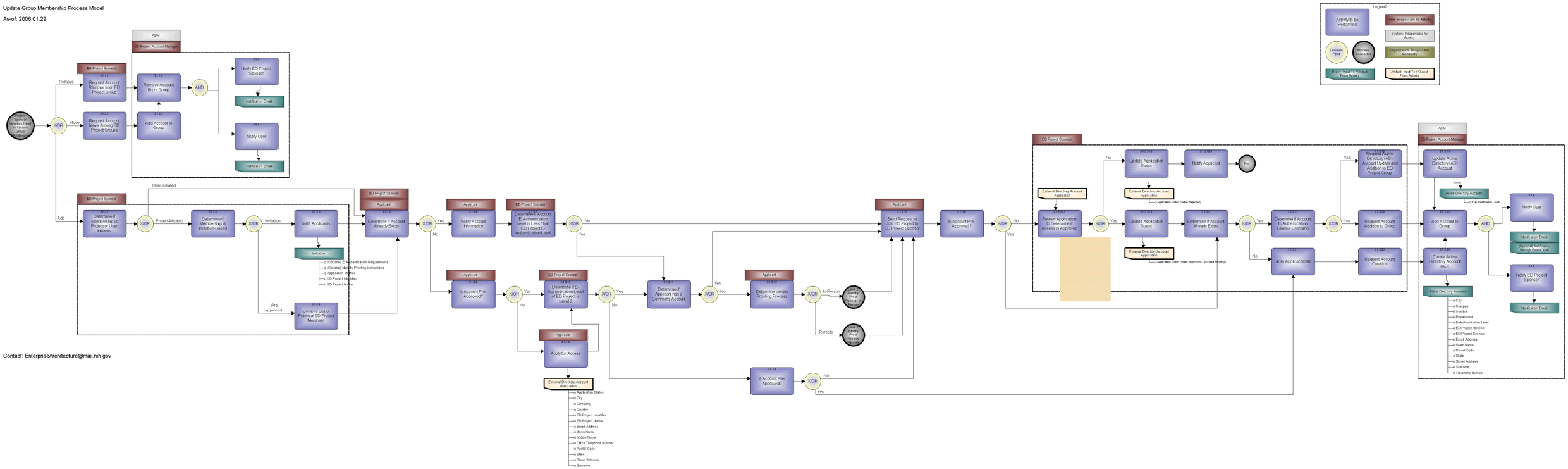
Contact: EnterpriseArchitecture@mail.nih.gov

Update Group Membership

External Directory

Update Group Membership Process Model

As-of: 2006.01.29



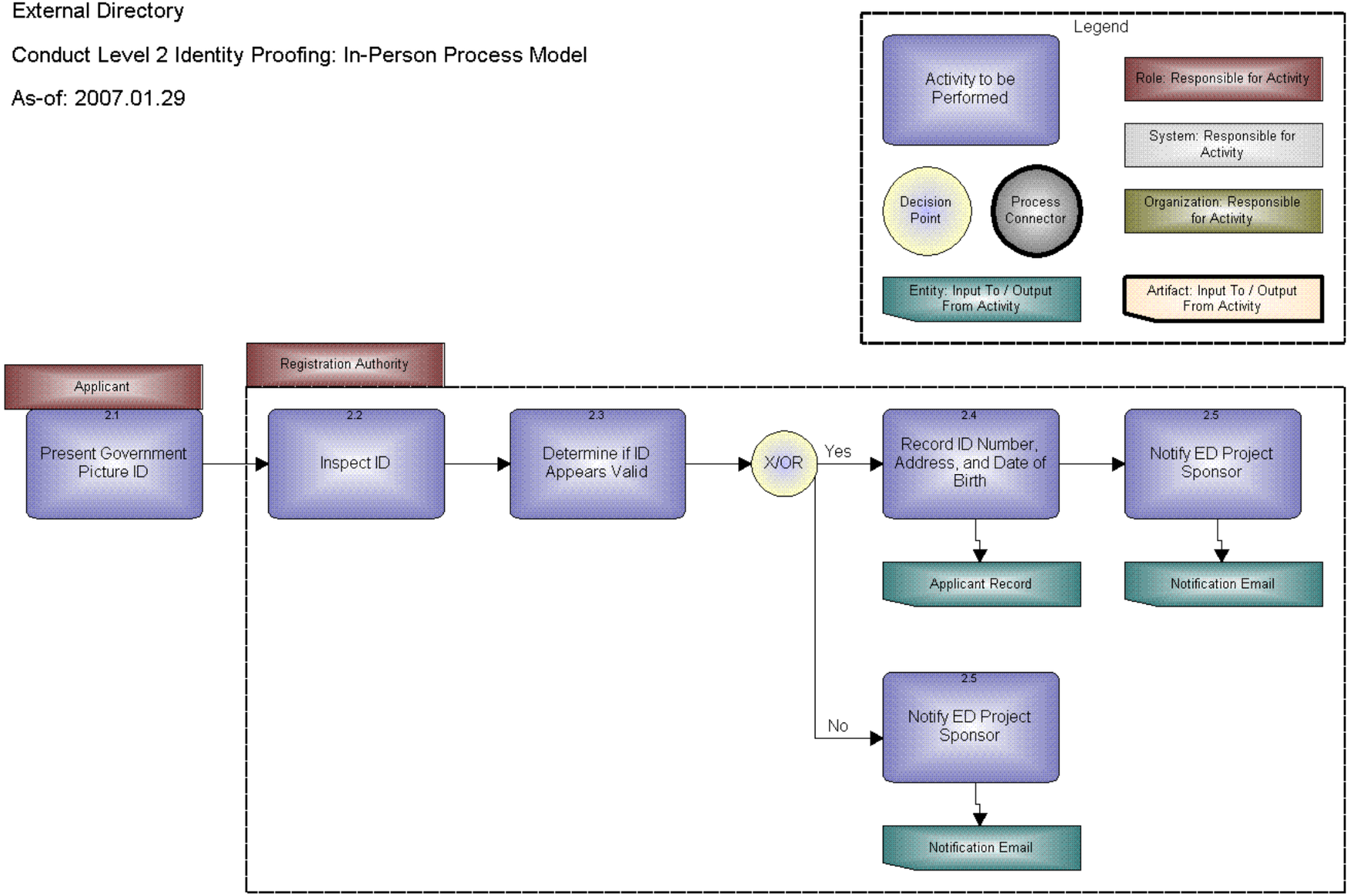
Contact: EnterpriseArchitecture@mail.nih.gov

Conduct Level 2 Identity Proofing: In-Person

External Directory

Conduct Level 2 Identity Proofing: In-Person Process Model

As-of: 2007.01.29



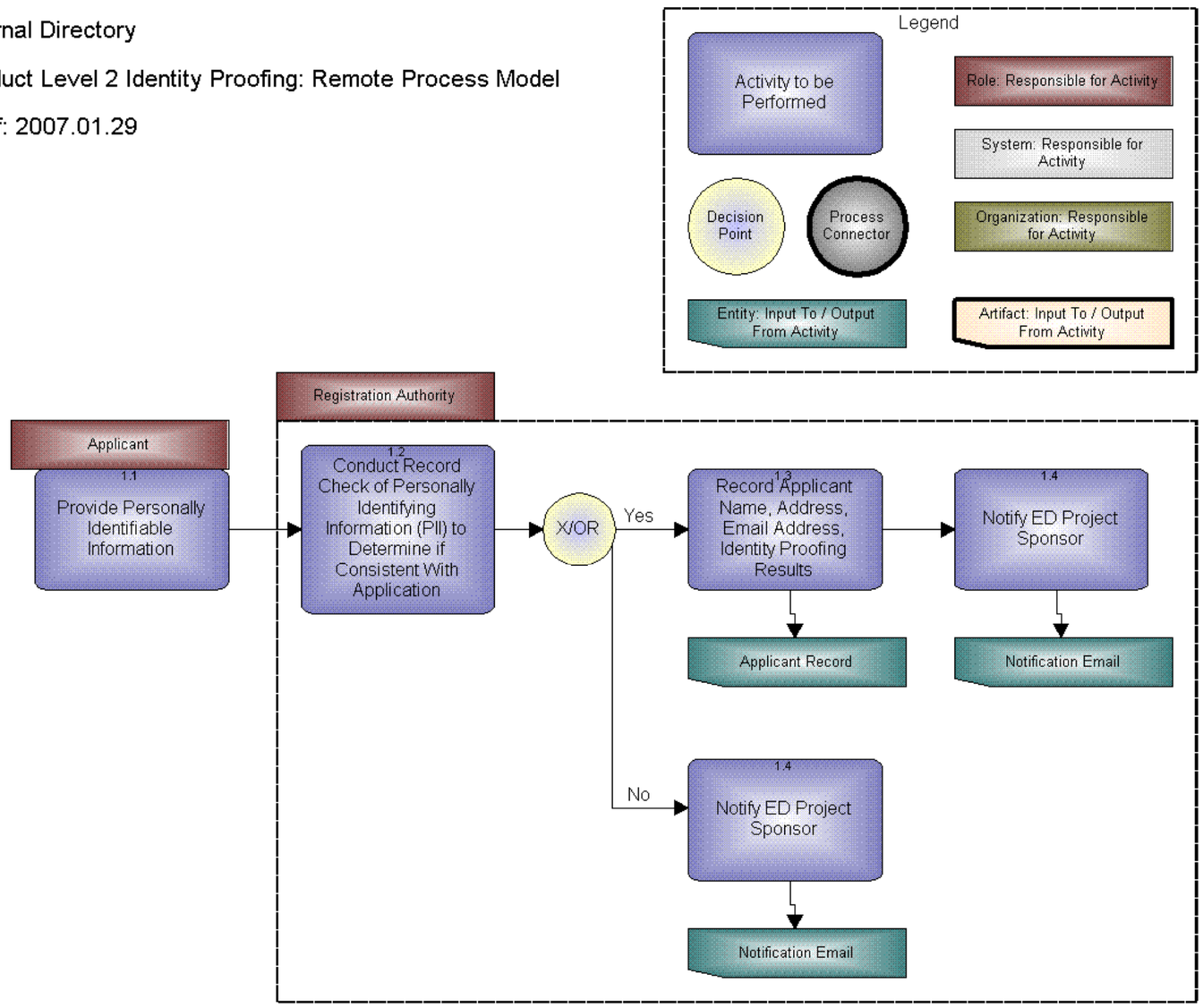
Contact: EnterpriseArchitecture@mail.nih.gov

Conduct Level 2 Identity Proofing: Remote

External Directory

Conduct Level 2 Identity Proofing: Remote Process Model

As-of: 2007.01.29



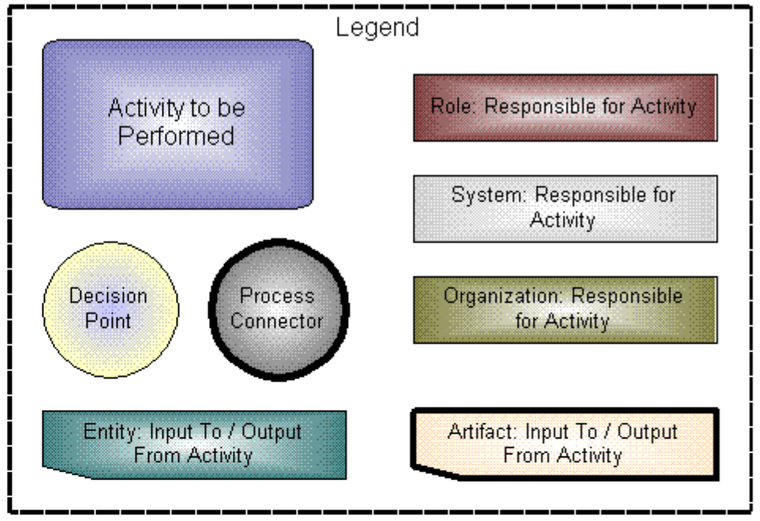
Contact: EnterpriseArchitecture@mail.nih.gov

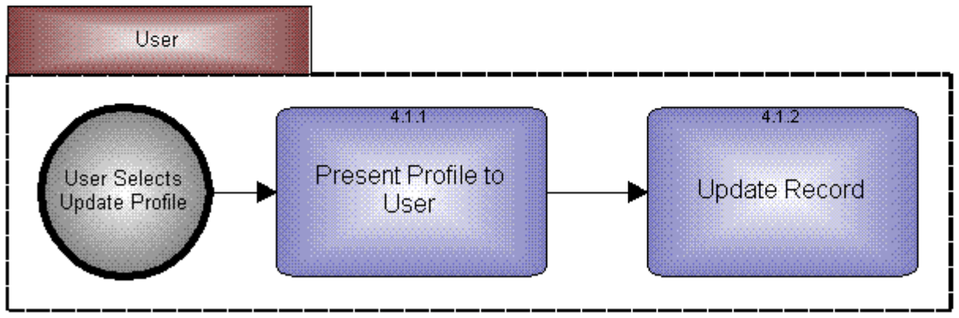
Update Account Profile

External Directory

Update Account Profile Process Model

As-of: 2007.01.29





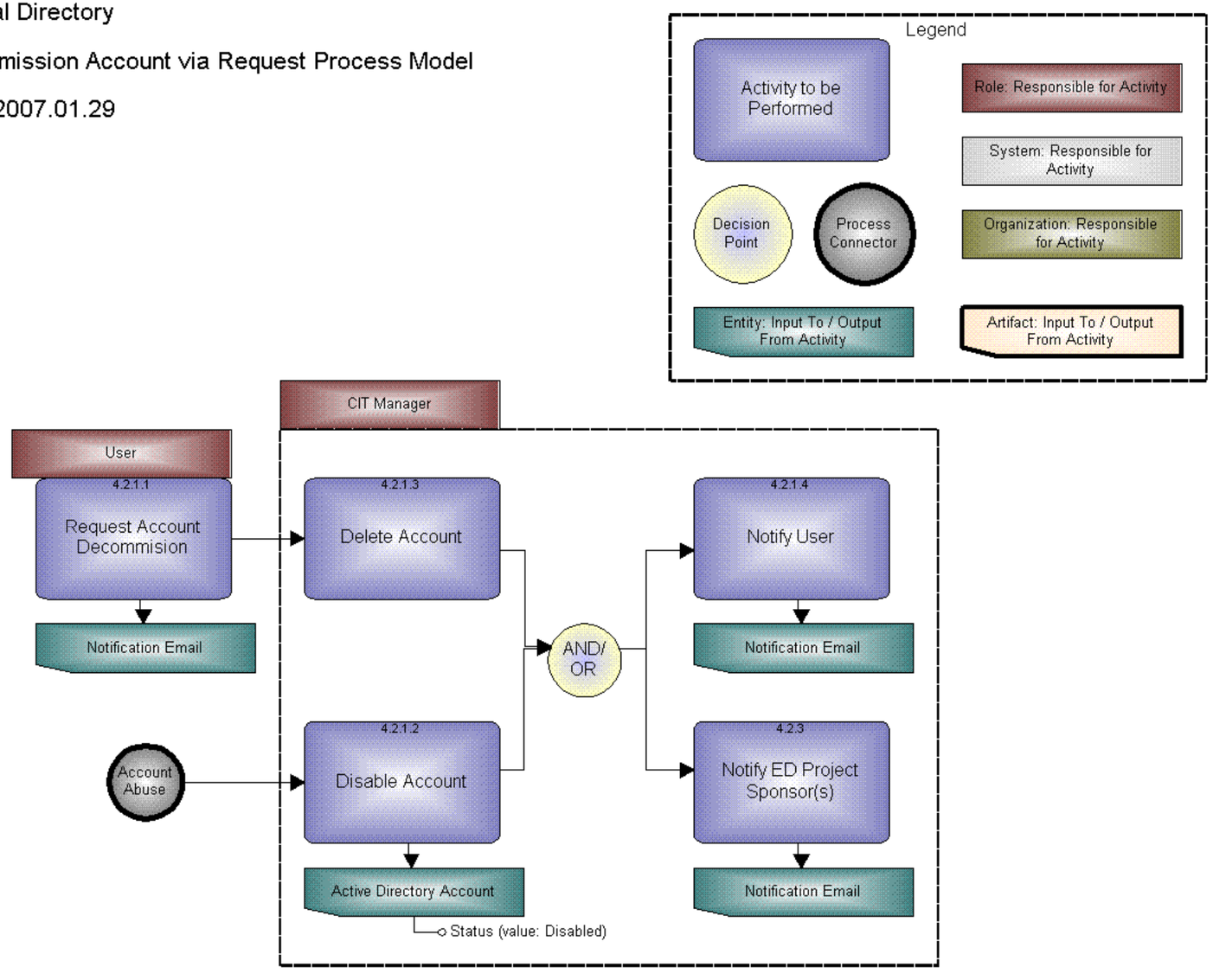
Contact: EnterpriseArchitecture@mail.nih.gov

Decommission Account via Request

External Directory

Decommission Account via Request Process Model

As-of: 2007.01.29



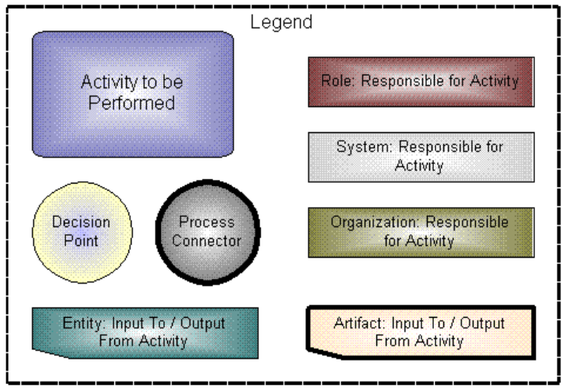
Contact: EnterpriseArchitecture@mail.nih.gov

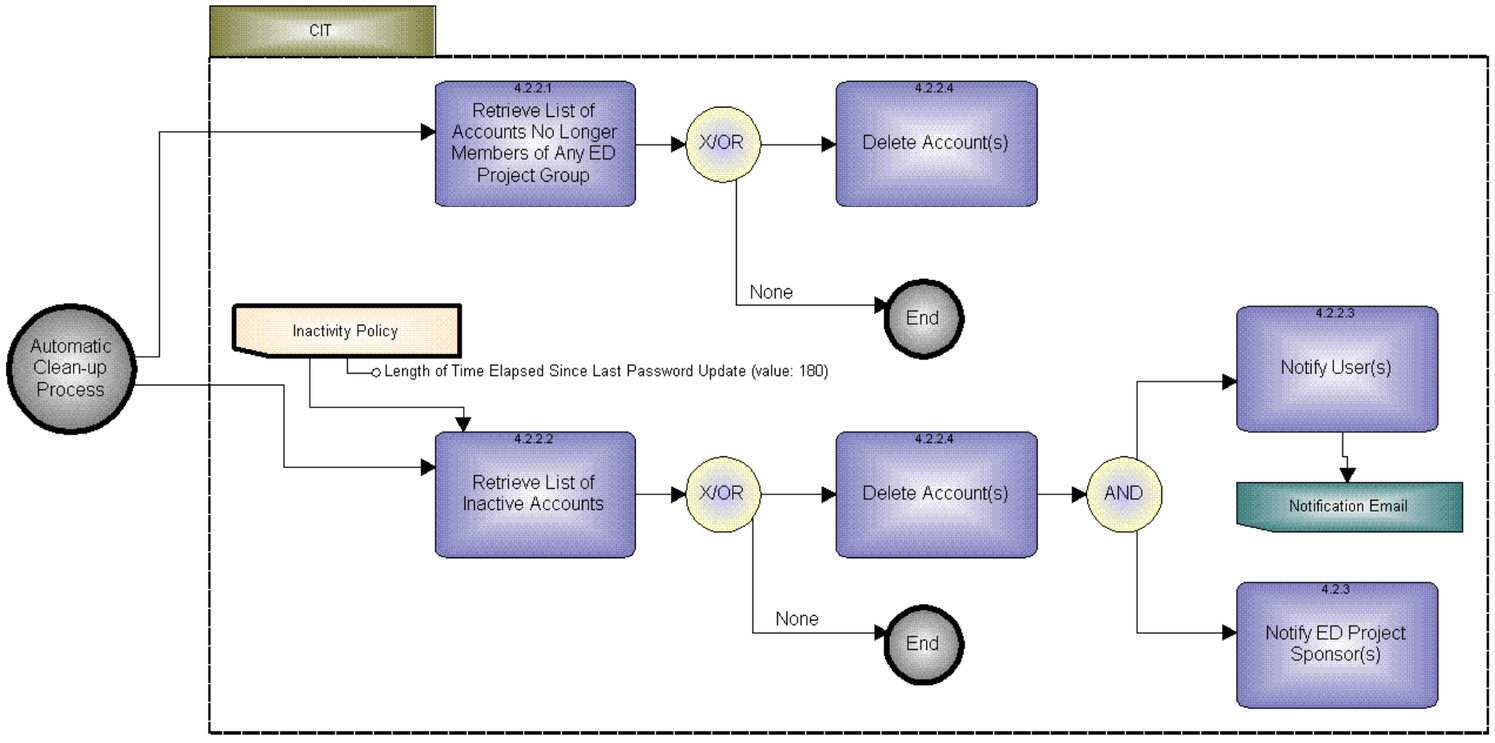
Decommission Account via Inactivity

External Directory

Decommission Account via Inactivity Process Model

As-of: 2007.01.29





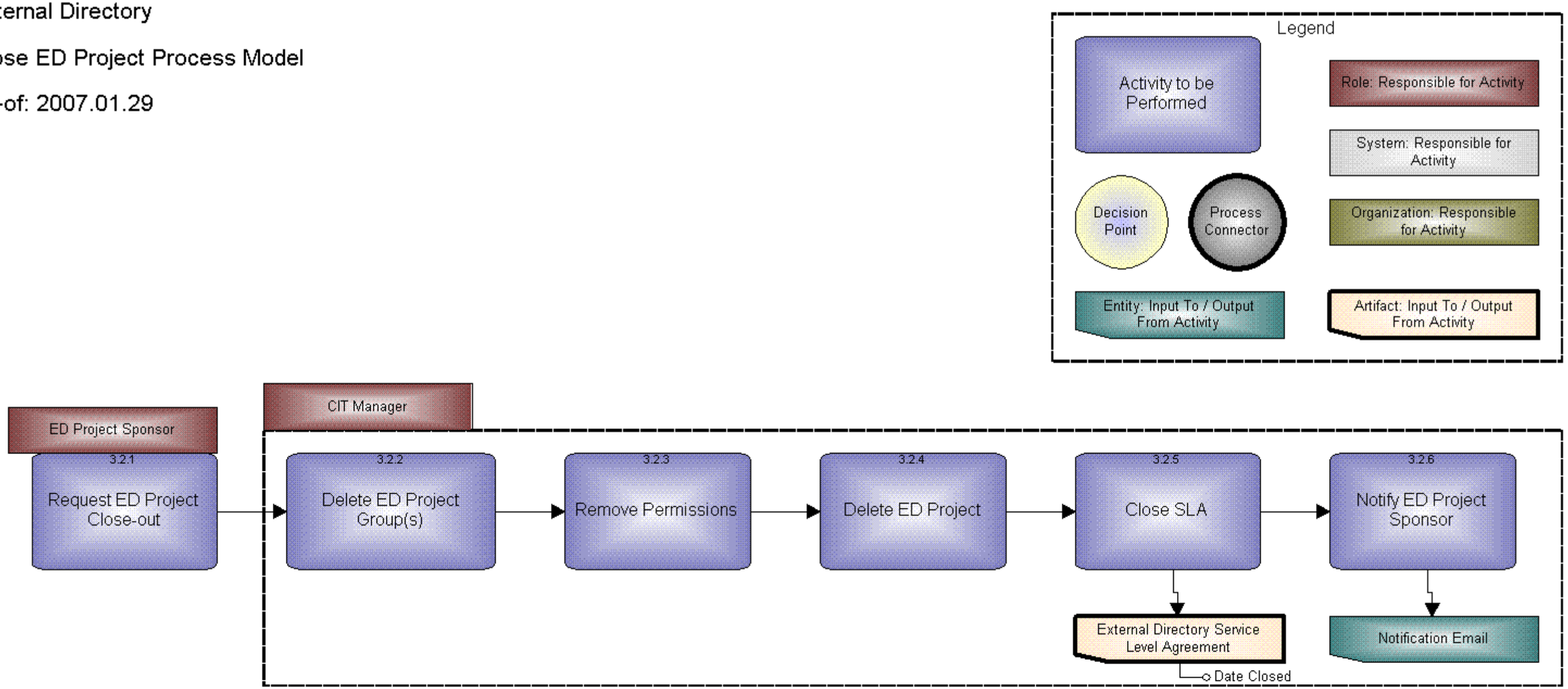
Contact: EnterpriseArchitecture@mail.nih.gov

Close External Directory Project

External Directory

Close ED Project Process Model

As-of: 2007.01.29



Contact: EnterpriseArchitecture@mail.nih.gov

Appendix II: Glossary of Terms

Term	Definition
Active Directory	An enterprise directory that lists and/or describes users and services on the NIH network and are typically used in conjunction with the enterprise messaging systems.
ADM Administrator	Individual responsible for activities related to the Active Directory
Applicant	Individual applying for access to NIH External
Center for Information Technology	Center for Information Technology that provides IT support to the 27 NIH ICs.
Document Management	Software systems that allow enterprises to generate, produce, store, manage, retrieve and distribute electronic files (e.g. text, image, audio, and video) yielding greater efficiencies in the ability to reuse information and to establish workflow constructs.
ED Project	System at NIH which requires external user access
ED Project Group	Collection of users within a project; used for authorization of users
ED Project Sponsor	Individual responsible for the project
Information System Security Officer	Identifies and implements standardized electronic security policies at NIH.
Organizational Unit	Container that logically stores directory information and provides a method of addressing Active Directory through Lightweight Directory Access Protocol (LDAP). It is the primary method for organizing user, computer, and other object information into a more easily understandable layout within Active Directory.
NIH External	External directory Active Directory solution at NIH
Personally Identifiable Information	Any pieces of information which can potentially be used to uniquely identify, contact, or locate a single person.
Registration Authority	Individual responsible for the identification of applicants, i.e. identity proofing
User	Non-NIH affiliated individual needing access to NIH systems; does not qualify to gain access through other NIH established processes
Virtual Private Network	Private communications network often used within a company, or by several companies or organizations, to communicate confidentially over a publicly accessible network.

Appendix III: References

1. Bolten, Joshua B., Director, Office of Management and Budget (OMB). *M-04-04: EAuthentication Guidance for Federal Agencies*.

2. http://enterprisearchitecture.nih.gov

3. http://irm.cit.nih.gov/nihsecurity/pwd_policy.doc

4. Burr, Bill; Polk, Tim and Dodson Dona; National Institute of Standards and Technology (NIST). *Special Publication 800-63: Electronic Authentication Guideline*

5. http://enterprisearchitecture.nih.gov/About/Approach/ProgramPlan2006Q1.htm

Change History

Date	Change Author	Change Authority	Change Event	Resulting Version
22 Sept 2006	Jae Lingberg	Helen Schmitz	Original Production	1.0
04 Feb 2007	Jae Lingberg		ARB recommendations incorporated.	1.1