DEAS Information Access Working Group
NRFC0019 / BCP0010
Category: Best Community Practice

S. Lozen
NIAID

March 2006

Division of Extramural Activities Support (DEAS) Central File Store Pattern v1.0

Status of this Memo

This memo provides a best practice for the NIH architecture community. This memo does not specify an NIH architecture standard of any kind. Distribution of this memo is unlimited.

Table of Contents

1 Introduction

1.1 Members

Central File Store pattern members/authors, by IC:

Schwartz, Andrew	CIT
Wampler, Valerie	CIT
Ingle, Joyce	CSR
Burke, Julie	FIC
McCullar, Alisa	FIC
Lee, Delores	NCRR
Richardson, Doane	NCRR
Robinson, Steven	NHGRI
Travers, Michelle	NHGRI
Walker, Fred	NHGRI
Smullen, Russell	NIA
Fleisher, Arne	NIAID
Kassing, Kim	NIAID
Lozen, Scott	NIAID
Brown, George	NIAMS
Connors, Anne	NIAMS
Wise, Matt	NIBIB
Klosky, Joe	NICHD
Bhatia, Manoj	NIDA
Yitbarek, Berhane	NIDA
LeVine, Rob	NIEHS
Simpson, Troy	NIEHS
Stegman, Nancy	NIEHS
Williams, Torraine	NIEHS
Waldman, Ivan	NIGMS*
Choi, Ruth	NIMH
Hermach, William	NIMH
Bond, Sandra	NINR
Koepke, Kathy	NINR
Bhandari, Rajesh	NLM

*NIGMS Conferred with the CFS chair and subsequently decided to pursue a different option.

1.2 Scope

Design a Central File Store based system to allow DEAS staff cross-IC information-sharing to support multiple ICs as required in their Basic Services Agreement.

1.3 Operating Principles

In designing and implementing this solution to providing DEAS staff access to IC information, the project team assumed the following:

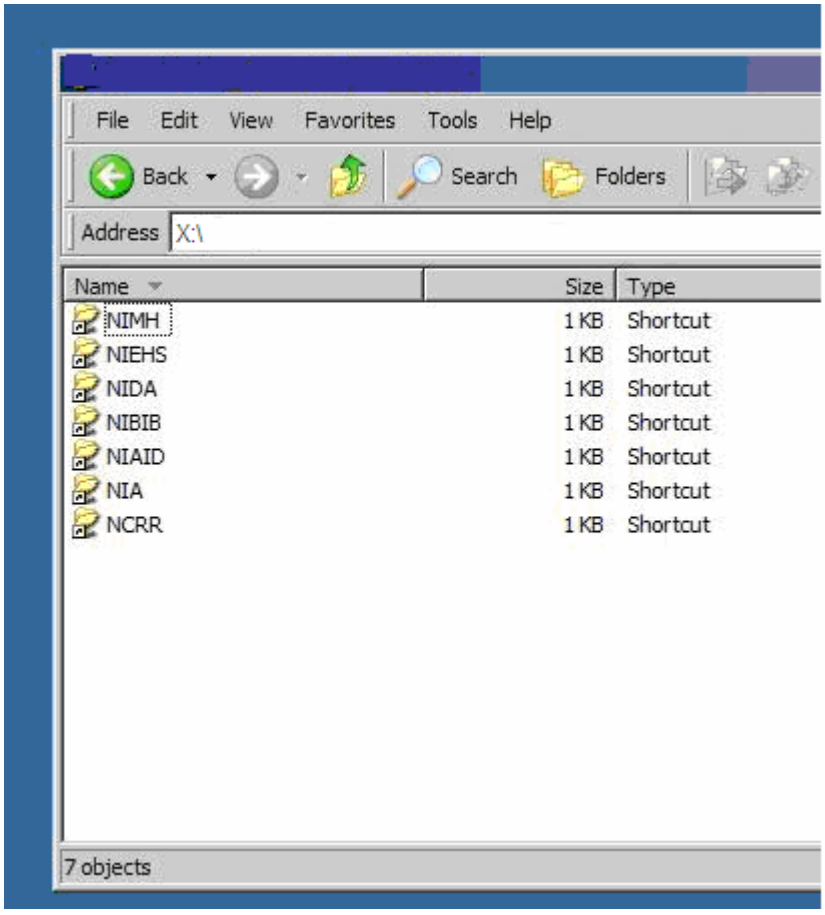
1. **Right to Assign Users to Roles** - DEAS task leaders will retain the right to assign job roles, not the IC.
2. **Data Ownership** - Information belongs to the Federal government not to any one organization (except information supplied as proprietary).
3. **Trustworthiness of NIH Staff** - All NIH staff members are assumed to be equally trustworthy.
4. **Role-Based Access** - Access to the information is based on the individual's assigned role, not other organizational criteria.
5. **Desktop Configuration** - All workstations meet the common NIH security standard.
6. **Active Directory** - Active Directory is the only mechanism for assigning users to roles and subsequently for affording access to file systems, based on a user's assigned role.
7. **HUB Configuration –** The DEAS hub structure is as specified in the DEAS Hub Structure (see Appendix B: DEAS Hub Structure).
8. **No Changes to Core IC Business Processes** - ICs will not be required to change core business processes (as opposed to system administration and automated assignment of roles) to accommodate the solution, which requires affordance of DEAS staff access to IC information and systems only, irrespective of geographic location or IC assignment. In other words, daily business operations for IC program staff will remain unchanged.
9. **Training Responsibility** - The cost and responsibility for developing and delivering training on the DEAS Information Access solution will be borne by the IC for IC staff and OD/DEAS for DEAS staff.

2 Technical Description

2.1 Central File Store Pattern

Division of Extramural Activities Support (DEAS) staff support all extramural research activities across NIH. DEAS staff may be required to serve more than one IC, from locations outside that IC. The proposed Central File Store Pattern presents a method of organizing file-based data that enables information access by DEAS staff working throughout the NIH community via one centralized menu for access to IC data.

This pattern provisions a central file server to store UNC links, essentially as menu items, to provide a single point of entry, or portal, to file based resources. See Picture 1: Central File Store



Picture 1: Central File Store

In the above depiction each Shortcut on the central menu system redirects to an IC managed folder structure assigned to the X: drive specifier. Use of a drive specifier is consistent with

practices already common within the NIH. Within this structure, ICs will assign permissions for folders and files to security groups. DEAS management will populate DEAS security groups.

The Central File Store server can be used to store data as well as links to IC file servers. The data and links would thus be co-mingled on the Central File Store server.

It is possible to build a more developed application to organize and mediate access to shared data via HTTP or WebDAV. This would require application design and development beyond the scope of this pattern.

2.2 NTFS Security Groups

Two specific approaches to NTFS security are identified below:

2.2.1 Standard Approach

Based on the manner in which ICs have structured their own Extramural organizations, the working group designed a paradigm of three security groups per DEAS hub as a standard:

- DEAS-HUBA-GRANTS
- DEAS-HUBA-PROGRAM
- DEAS-HUBA-REVIEW

- DEAS-HUBB-GRANTS
- DEAS-HUBB-PROGRAM
- DEAS-HUBB-REVIEW

- DEAS-HUBC-GRANTS
- DEAS-HUBC-PROGRAM
- DEAS-HUBC-REVIEW

2.2.2 Alternate Approach

The Center for Scientific Review (CSR) requires a more granular security group structure, detailed below:

- NIH OD DEAS CSR ONSITE

- NIH OD DEAS CSR OFFSITE AARR
- NIH OD DEAS CSR OFFSITE EMNR
- NIH OD DEAS CSR OFFSITE IDM
- NIH OD DEAS CSR OFFSITE IMM

- NIH OD DEAS CSR OFFSITE ONC
- NIH OD DEAS CSR OFFSITE BCMB
- NIH OD DEAS CSR OFFSITE BDA
- NIH OD DEAS CSR OFFSITE BST
- NIH OD DEAS CSR OFFSITE CB
- NIH OD DEAS CSR OFFSITE GGG
- NIH OD DEAS CSR OFFSITE MDCN
- NIH OD DEAS CSR OFFSITE CVS
- NIH OD DEAS CSR OFFSITE DIG
- NIH OD DEAS CSR OFFSITE HEME
- NIH OD DEAS CSR OFFSITE IFCN
- NIH OD DEAS CSR OFFSITE MOSS
- NIH OD DEAS CSR OFFSITE RES
- NIH OD DEAS CSR OFFSITE RUS
- NIH OD DEAS CSR OFFSITE BBBP
- NIH OD DEAS CSR OFFSITE BDCN
- NIH OD DEAS CSR OFFSITE HOP
- NIH OD DEAS CSR OFFSITE RPHB
- NIH OD DEAS CSR OFFSITE SBIB

CSR Offsite roles would be limited to 2 month duration and would not have delete privileges.

2.3 IC ISSO Review

IC ISSOs may review DEAS security group membership and contact DEAS management to request modifications as appropriate.

2.4 Implementation Tasks

2.4.1 Shared Drive Letter

The working group has conducted a survey to determine an appropriate drive specifier. Drive letter x: was determined to be the most available drive specifier. NIDA was using this drive specifier, but has graciously agreed to make it available for the Central File Store.

Where the X: drive specifier is not available it is permissible for ICs to designate another letter. The inconsistency risks communications difficulties as IC and DEAS staff refer to document locations.

There is no requirement that ICs use X:, or any drive spcifier for providing access to IC folder structure for their own staff. The inconsistency risks communications difficulties as IC and DEAS staff refer to document locations.

Level of effort: Low to moderate.

2.4.2 Logon Script

DEAS staff will use a logon script to gain access to mapped drives. Where DEAS staff use IC logon scripts, IC logon scripts will be changed as appropriate to accommodate the new drive mapping.

Level of effort: None to Moderate
Responsibility: IC technical staff

2.4.3 File Server

ICs shall make DEAS accessible resources available through their firewalls. As necessary, IC firewall rules shall be modified. If necessary, DEAS accessible resources shall be located in a DMZ. The CIT offers hosting solutions for those who do not prefer to host the data themselves.

As appropriate, participating ICs shall ensure that file server(s) are registered with NIH Active Directory Dynamic Domain Name Service (DDNS) to allow accessibility across NIH.

Level of effort: None to Low
Responsibility: IC technical staff

2.4.4 Provision Permissions to IC resources

IC technical staff shall apply the NTFS group permissions to the resources which are to be made available to DEAS users.

Level of effort: Moderate
Responsibility: IC technical staff

2.4.5 Provision Central File Store

CIT technical staff shall provision a central file store to store UNC links, essentially as menu items, to provide a single point of entry, or portal, to file based resources, as described in 2.1. All DEAS staff and appropriate IC staff shall have read permission to this first level CFS menu. IC technical staff shall have the ability to modify this first level CFS menu.

Level of effort: Low
Responsibility: CIT technical staff

2.5 Risk Analysis

2.5.1 Acceptance

Risk: There is a risk that organizations (IC or program areas) will not want to accept the solution defined by the project team.

Mitigation: Team members are updated regularly. Feedback is solicited and where appropriate, incorporated into the project plan.

2.5.2 Adoption of recommended drive specifier

Risk: ICs may decide to use their current drive mappings instead of the recommended drive specifier.

Should this occur, communication problems between the IC and DEAS individuals are possible. For example, the IC individual may refer to a document on his/her G: drive, while the DEAS individual will refer to the document being on his/her X: drive. Links embedded in email may not function correctly.

Mitigation: ICs are strongly encouraged to change drive mappings to match the DEAS Central File Store X: drive mapping,

2.5.3 Security

Risk: DEAS users assigned to more than one hub group.

Mitigation: IC ISSOs to have oversight authority on group membership. DEAS task managers shall coordinate with ISSOs to remediate duplicate memberships.

2.5.4 Training

Risk: DEAS users and IC staff must receive accurate, timely training on the use of the CFS.

Mitigation: Responsibility for training has been assigned to the IC for IC staff and to OD/DEAS for DEAS staff.

3 References

There are no references for this NRFC.

4 Contact

To contact the NRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov.

5 Security Considerations

The CFS implementation must include adequate security measures to ensure data integrity through enforcement of authentication and authorization, adequate physical security of hardware, as well as network connectivity that complies with security regulations and guidelines. ICDs may implement auditing for the level of accountability appropriate for their business model.

6 Changes

Version	Change	Authority	Author of Change
0.0	Original NRFC	Author	Scott Lozen/ DEAS.CFS working group
0.1	Post-presentation modifications	Author	Scott Lozen/ DEAS.CFS working group
0.2	Responses to online comments	Author	Scott Lozen
	Section 2.1		
	Section 2.4.1		
	Section 2.4.2		
	Section 2.5.2		
1.0	(1) Applied date of approval and administrative changes to header (2) Corrected table of contents (3) Corrected status of this memo	NRFC0001	Steve Thornton, NRFC Editor

7 Author's Address

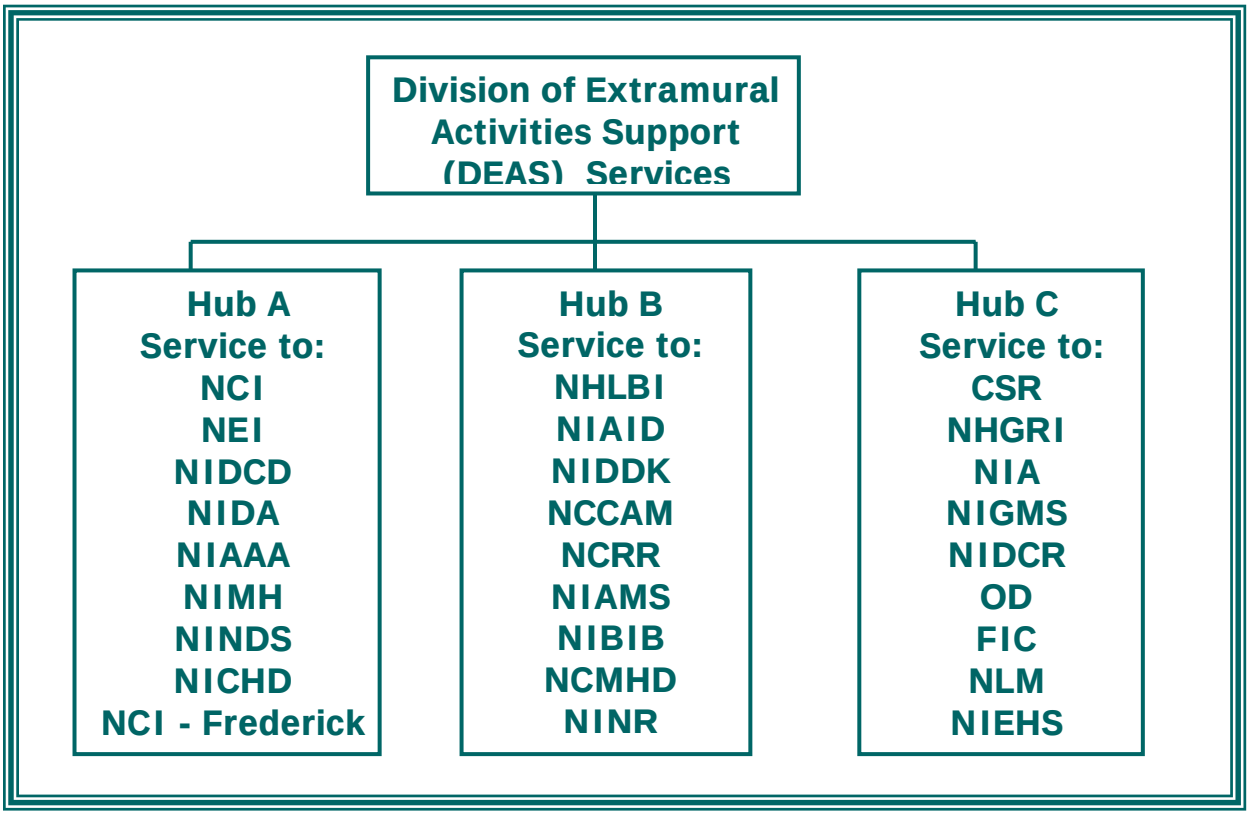
Scott Lozen
National Institutes of Health
10401 Fernwood Road
MSC 4819
Bethesda, Maryland 20817
Phone: 301-402-3580
Email: slozen@mail.nih.gov

Appendix A: Appendix A: Drive Specifier (Letter) Responses

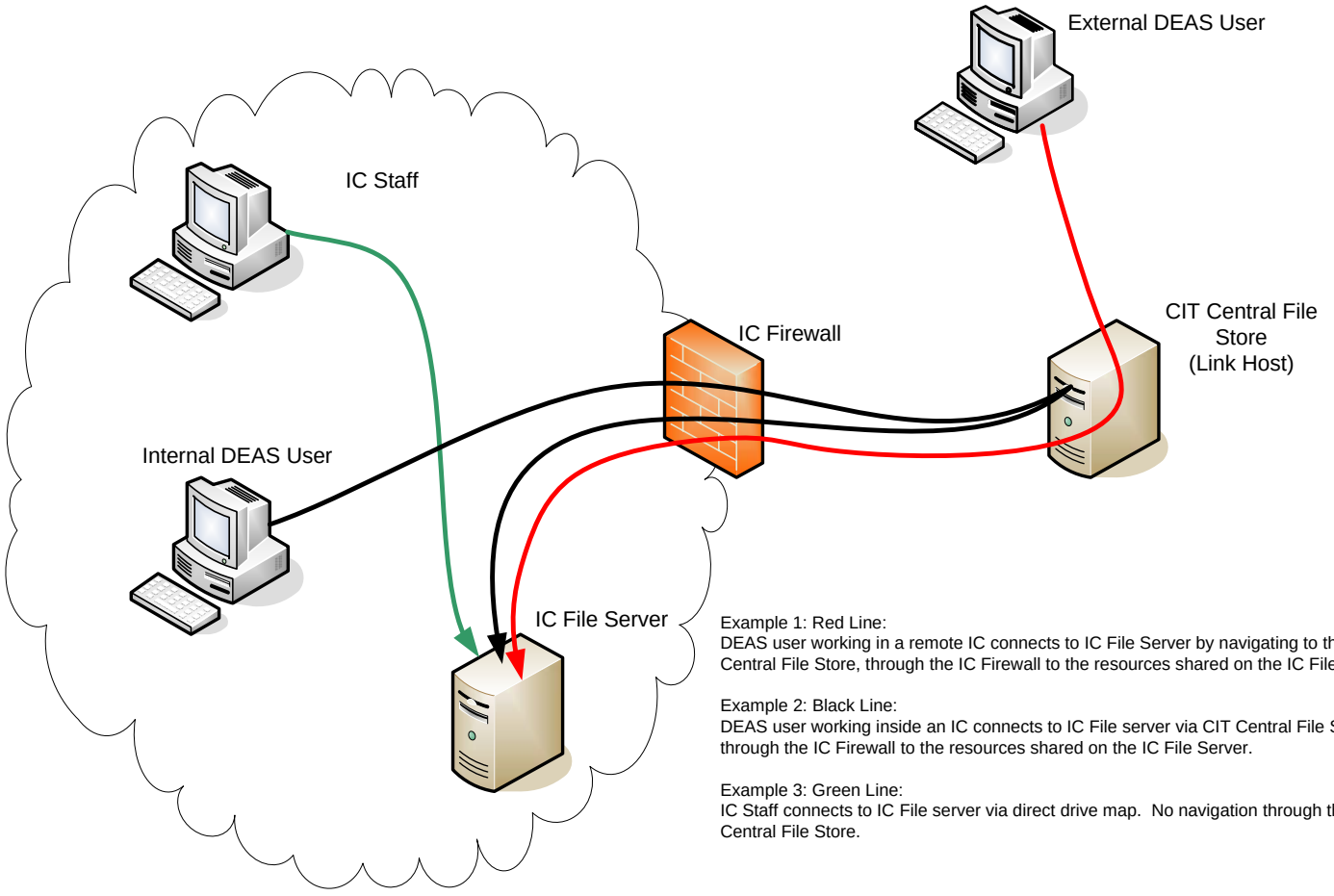
ICD	Responded	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CSR	Ingle, Joyce (NIH/CSR)	1	1									1				1			
FIC	Burke, Julie (NIH/FIC)											1	1		1				
NCRR																			
NHGRI	Travers, Michelle (NIH/NHGRI)		1	1	1						1	1	1			1			1
NIA	Smullen, Russell (NIH/NIA)									1		1	1			1			
NIAID	Lozen, Scott (NIH/NIAID)			1						1	1	1	1	1					
NIAMS	Brown, George (NIH/NIAMS)						1	1	1	1	1	1	1		1				
NIBIB	Wise, Matt (NIH/NIBIB)				1		1		1			1							
NICHD	Klosky, Joe (NIH/NICHD)						1		1				1						
NIDA	Yitbarek, Berhane (NIH/NIDA)		1		1		1	1	1	1	1	1	1	1	1	1	1	1	1
NIEHS																	**0**		
NIMH	Hermach, William (NIH/NIMH)	1	1	1	1	1	1	1	1	1	1	1	1						
NINR	Bond, Sandra (NIH/NINR)	1			1	1	1		1		1					1		1	1
NLM																			
14	11	3	4	3	5	2	6	3	6	5	6	9	8	2	3	5	1	2	3

Appendix B: Appendix B: DEAS Hub Configuration

Note: this Hub structure is currently under review by OD management:



Appendix C: Appendix C: Architectural Diagram



Example 1: Red Line:
DEAS user working in a remote IC connects to IC File Server by navigating to the CIT Central File Store, through the IC Firewall to the resources shared on the IC File Server.

Example 2: Black Line:
DEAS user working inside an IC connects to IC File server via CIT Central File Store, through the IC Firewall to the resources shared on the IC File Server.

Example 3: Green Line:
IC Staff connects to IC File server via direct drive map. No navigation through the CIT Central File Store.

Appendix D: Appendix D: Notes from Dec. 20, 2005 presentation

1. It is possible to use a web page with links to file shares as an alternative to mapping DEAS individuals to an X: drive. However, this approach would require keeping the Web page in sync with the drive changes within the ICs, so that the correct drives are consistently displayed.

2. It was noted that it is possible to restrict access to parts of an IC file share tree structure while having other parts of the tree un-restricted.

3. Valerie Wampler has proposed a solution for DEAS security groups that has IC security groups nested within newly created DEAS security groups. This solution would allow the "most restrictive" group protection of a file share to "win", giving ICs greater control over their file share data while allowing DEAS staff the necessary access to accomplish their tasks.

4. OCITA has collected security groups that ICs use to protect their file share data. It may turn out that we need to create new DEAS security groups that mirror all of the IC security groups. In other words, it may not be as simple as creating DEAS-MyIC-Program, DEAS-MyIC-Review and DEAS-MyIC-Grants security groups. The DEAS supervisors will need to understand the purposes of all of the new security groups so that they will be able to determine which group(s) to place a DEAS individual into in order for that DEAS individual to accomplish his/her tasks. More analysis and conversations with the business need to occur before groups are created to determine how much, if any, standardization can be accomplished.