



## Interagency Interoperability Oversight Group

### Access Authentication (One Desktop) – Alternative Solution Workshop Solution Brainstorming Session



#### Problem: Collaborative - Location of Shared Data / File Storage

**Solution Alternative 1 - Cloud** provided like Box (similar to drop box but designed for enterprise use and security controls) – Scheduled to be FedRAMP Certified by end of Calendar Year. Google is another option.

Criteria	Explanation
Level of Effort	1a Permissions Management: High 1b Permission Management: Lower than 1a
Resources / Cost	Start Up: Low to Moderate Annual: Low to Moderate
Timeframe / Implementation	*Dependent upon the contracting process. 1b Security
Security	Is separate C and A required? 1a – Low 1b – Moderate to High
Pros	1a – Isolated/Stand-alone solution provides for business needs but not linked to other systems; so reduces complexity and cost for implementation.  -No duplication of equipment needed. One workstation on a single user's desk.
Cons	Access Management complex. No longer have access to local resources. Data will likely be duplicate in enterprise systems and here. 1a and 1b – no messaging services (depending upon vendor).
Non-Fed Cooperator Access	Enabled but w/o messaging services (dependent upon vendor). Shared place to place and retrieve information.

**Additional Information Needed to Examine Option:** \*How many SEATS potentially, must be scalable as demand grows.

#### Implementation Concerns:

1a - No ADFS

1b – Use ADFS will have integration effort but easier to manage permissions over long term.

**Solution Alternative 2 - Active Directory Forest Trust** – Two departments trust each other. Widest access available. Map printers.

Criteria	Explanation
Level of Effort	Technically: Low Security: Moderate to High
Resources / Cost	Lowest Cost Alternative - If a considerable amount of traffic occurs, it may take a separate network to facilitate. Network infrastructures will need to be addressed to ensure adequate capacity.

Criteria	Explanation
Timeframe / Implementation	Easy technically to implement (hours, not days) for AD resources/applications. However, would need to migrate O-Drive, etc., resources/applications to AD credentialed area. Sharepoint could provide solutions.
Security	<p>Must define how to respond to security incidents, tighter coordination of security efforts between all.</p> <p>Both agencies use USA Access, which standardizes user account creation and association.</p> <p>No permission management overhead; except WHO within DOI to FS and vice versa.</p>
Pros	<p>Provides the widest access to AD aware network resources, fairly easy to implement technically.</p> <p>MOU for Interagency Recognition of Security Controls and Credentials already in place at DOI/USDA level.</p> <p>Printers could be mapped as they are AD aware. May not resolve thin print instances.</p>
Cons	<p>Most difficult to implement from a security and <b>politics</b> standpoint.</p> <p>Does not provide access content DB, O-Drive, Oracle Internet Directory, OID, etc.</p> <p>Ads a level of complexity when using joint resources because it can be confusing when trying to get fixed, updated, etc. This requires additional coordination to facilitate sharing. (removing printers, etc. for example)</p>
Non-Fed Cooperator Access	Most flexibility in that each agency/bureau already provisions for this.

**Solution Alternative 3 - ADFS Capability / Brokerage** to an internally hosted collaboration site in either Forest. One would host, the other would provide ADFS credential.

Criteria	Explanation
Level of Effort	Mod for everyone to setup ADFS structure. Allow to validate and allow users access.
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	WE don't need a purpose build on premise of SharePoint, but rather expand existing sharePoint capabilities. Could be less costly than the Cloud.
Cons	
Non-Fed Cooperator Access	
Additional Notes:	Capacity of ADFS could be additional requirement. What is the value of ADFS? Can be connected to e-Auth...integrate with Apps. No shared of resources, such as printing. Who will manage, USDA or DOI? ADFS is a "connector" and an "enabler", but doesn't resolve all things. Messaging and Collaborations is much more important than printing.

**Problem - Access & Authorization to Other Applications**

<b>Criteria</b>	<b>Explanation</b>
Level of Effort	
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	

**Problem - Access and Authorization to Applications - Paycheck, GovTrip**

<b>Criteria</b>	<b>Explanation</b>
Level of Effort	
Resources / Cost	
Timeframe / Implementation	Chris Moyer will work with Omar Thompson on this. Need issue paper.
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	Need to work with HRM to get interagency process approvals in place.

*Reminder sent 6/10/2013*

**Problem - Specific Locally Hosted Applications (WildCAD)**

<b>Criteria</b>	<b>Explanation</b>
Level of Effort	
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	

### Problem - Simultaneous Email Access

**Issue:** Dispatchers and Service First employees need to access both (DOI) BLM and FS email via one desktop. This works for accessing DOI gmail but not for access to USDA email.

Criteria	Explanation
Level of Effort	Not asking for open to internet but open to DOI.
Resources / Cost	
Timeframe / Implementation	Doug/Clint will discuss week of 5/27 at USDA
Security	Politics of DOI opening email to USDA and vice versa. A security mitigation policy disallowed email to USDA from internet. Can ASOC be convinced that this should be done?
Pros	This is a tradeoff between business requirement and acceptable risk.
Cons	
Non-Fed Cooperator Access	Unless they have access to one or the other networks there will be no access.
Additional Notes:	Doug Nash in support of working toward resolution with USDA ASOC. Clint Swett will assist in talking with Chris Lowe on this.

**NEED TO REMEMBER:** Some things that are being done through email could be done through alternative approaches such as posting to a website and how it gets exposed and shared and how workflow gets handled. Need not to look to email as the only solution.

### Problem - Shared Email for Initial Attack Dispatch (vice DMS)

Criteria	Explanation
Level of Effort	
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	

**Problem - Shared Expanded Dispatch Email (for travel arrangements, etc.)  
Shared Email for Service First Applications**

Implementation is not always consistent between DOI / BLM State Offices and FS (managed accounts).

Criteria	Explanation
Level of Effort	Difficult since one email acct is not possible
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	One email base solution is not possible – an additional email acct will be needed. Requirement for a joint email acct to monitor from such an email acct....need to solve size limitation and bringing in outsiders. 3 <sup>rd</sup> acct where we can manage and monitor the email system. DMS maybe replaced by gmail. Gmail setup at DOI is through AD.

**Problem - Shared AD Directories**

DOI and USDA need to do periodic exports to provide a list where employees look up addresses. Put it into email system. Outlook has the capability. DOI does not have a GAL. They have a limitation in the number of contacts that we can store outside of employee directory information in Google. Can export one department-wide employee directory. There needs to be an automated method pulled together to make this happen.

Criteria	Explanation
Level of Effort	
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	

**ACTION:** POC from USDA – Clint Swett, and POC from DOI – Pat Price and Andrew Havelly will spearhead; will work together to see what is necessary to facilitate this. Cost in time, ability to implement. Can you do, how hard is it manual and what would it take to automate it?

**Report Back:** First week of June  
(reminder sent 6/10/2013)

**Problem – Sharing Other Network Devices (printers, NAS, etc.)**

Criteria	Explanation
Level of Effort	
Resources / Cost	

<b>Criteria</b>	<b>Explanation</b>
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	Dependent upon a full AD trust environment to make this work.

**Problem - External non-Federal Account Access**

<b>Criteria</b>	<b>Explanation</b>
Level of Effort	
Resources / Cost	
Timeframe / Implementation	
Security	
Pros	
Cons	
Non-Fed Cooperator Access	
Additional Notes:	