



Interagency Interoperability Oversight Group



Access Authentication

Solution Team Report and Recommendation

Interagency Access Authentication Project Team

11/6/2013



Interagency Interoperability Oversight Group Access Authentication Solution Team Report and Recommendation

Executive Summary

The Access Authentication project was initiated in May 2009 by the Interagency Interoperability Oversight Group (IIOG). The project scope included the development of a method to allow Department of the Interior (DOI) or Forest Service (FS) employees a simple and efficient way to access Information Technology (IT) resources and applications appropriate to their duties, regardless of employing agency. To date, multiple challenges have made it impossible to provide this capability to the field. In April 2013, an interagency team representing the US Department of the Interior (DOI), Bureau of Land Management (BLM), US Department of Agriculture (USDA) and Forest Service (FS) were directed by the Wildland Fire Information and Technology (WFIT) Executive Board to:

- Re-validate the business need for DOI and FS users to efficiently access each other's networks/applications
- Develop a recommended solution that meets customer needs and maintains network security processes for all agencies.

Team representatives included technical subject matter experts from USDA, DOI, BLM and FS and business representatives from Fire and Aviation Management and Service First Program Management. All decision points were fully vetted with the team and recorded. A team consensus was validated prior to moving forward during each phase of the analysis.

Collaboratively the team identified four options; however, each option individually offered solutions to only a portion of the business needs. The team found that the majority of business needs could be met by combining the options to create four alternatives. The four alternatives include:

- Alternative 1 - One AD/Network w/External Public Cloud.
- Alternative 2 - DOI / USDA Inter-Forest Trust w/External Public Cloud
- Alternative 3 - One AD/Network w/Internal Cloud Hosted by One Agency Only.
- Alternative 4 - DOI / USDA Inter-Forest Trust w/Internal Cloud Hosted by One Agency Only.

Each alternative was rated against **value** factors as described below:

- End User Value: Benefits to customers/clients, for example, convenient access, product enhancement.
- Operational Value: Better operations and lowering barriers to future initiatives, for example, improved infrastructure
- Strategic/Political Value: Contributions to strategic initiatives and fulfilling the mission of the organization
- Social Value: Benefits to society as a whole

The team measured each alternative in terms of **risk** as defined by OMB in their Circular A-11.

While the team was not able to analyze **costs** in terms of actual dollars spent on each major component involved (i.e., Telecommunications, servers, software, licensing, contractual costs, etc.), the team measured costs in terms of capital outlays.

Quick Wins and recommended other actions outside the scope of this project were also identified to further assist in providing better interagency access for users.

Upon management decision on which approach to adopt and implement, a full project plan needs to be developed. It is estimated that with proper resourcing and management priority that a full solution set can be available to the user community within one year.

Summary - The interagency project team collaboratively and unanimously agree that the recommended alternative is Alternative 2 - DOI / USDA Inter-Forest Trust with Externally Hosted Public Cloud.



Interagency Interoperability Oversight Group
Access Authentication Solution Team Report and Recommendation

Table of Contents

Executive Summary..... i

Table of Contents.....iii

1. Background..... 1

2. Team Members2

3. Approach3

4. Alternatives4

 Alternative 1 - One AD/Net w/External Public Cloud.....4

 Alternative 2 - DOI / USDA Inter-forest Trust w/External Public Cloud5

 Alternative 3 - One AD/NET w/Internal Cloud Hosted by One Agency Only.....6

 Alternative 4 - DOI / USDA Inter-Forest Trust w/Internal Cloud Hosted by One Agency Only7

5. Quick Wins.....8

6. Next Steps / Additional Recommended Actions.....8

Appendix A – Value Analysis.....9

Appendix B - Risk Analysis13

Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed16

Appendix D - Summary of USDA / DOI Risk and Value Assessment for Solution Alternatives17

Attachment 1 – Detailed Analysis Calculations and References18



Interagency Interoperability Oversight Group

Access Authentication Solution Team Report and Recommendation

1. Background

The ability to log-on to a the Forest Service or Department of the Interior (DOI) network efficiently, while easily accessing applications regardless of employing agency, has been a critical business need identified by employees located in interagency offices throughout the nation for nearly 20 years. This need has also commonly been referred to as single sign-on and one-desktop. Because no other group or organization had been able to find and implement a workable solution to date, the IIOG chartered this project in May of 2009 and updated the charter in November of 2010. Those charters and associated project materials are available on the [IIOG Website \(http://www.IIOG.gov\)](http://www.IIOG.gov). Resource availability, changes to IT security policies and other related issues has continued to prohibit completion of this project. In April 2013 the IIOG and newly formed Wildland Fire Information and Technology (WFIT) Executive Board¹ directed that the project team work again toward a solution. Meetings began in April 2013 and have continued in order to deliver this analysis and report for management consideration.

Key business needs include three primary categories:

Category 1 – The need for USDA and DOI government employees to be able to securely collaborate and work together, regardless of their location. This includes the ability to efficiently access network, applications and peripherals associated with duties, regardless of agency affiliation or network ownership.

- The ability to access email from any computer located at the employee workstation must be facilitated.
 - There are times that it becomes necessary for a fire dispatcher to leave their workstation to check agency specific email. Dispatchers in the course of their daily work are not allowed to leave their work area without positive hand off of their responsibilities to another dispatcher; despite the fact that another dispatcher may not always be available. This leaves email unread.

Category 2 - The need for both/either Department to collaborate and interact with non-Federal public/state/private entities. For example, the ability to share large documents, files and email with Federal and Non-Federal employees associated with incident management. Shared email capability (short-term) in support of an incident; including non-Federal participants.

- Shared email capability (long-term) for each dispatch office.
- Shared email capability (short-term) for incident management and expanded dispatch.

Category 3 – Business Needs outside the scope of the project.

- For example supervisory ability to approve timesheets, travel, etc., for employees regardless of employing agency association.

¹ The WFIT was chartered and signed August 8, 2012 by Kim Thorsen, Deputy Assistant Secretary – Public Safety, Resource Protection and Emergency Services, Department of the Interior and Jim Hubbard for Arthur Blazer, Deputy Under Secretary Natural Resources and Environment, US Department of Agriculture. Jim Hubbard, Deputy Chief, State and Private Forestry, USDA Forest Service and Kim Thorsen serve as co-chair.

2. Team Members

Team members included representatives from the USDA, FS, DOI, International Technology Services (ITS), and the Bureau of Land Management (BLM). While not all members were able to attend each meeting, no decisions toward a team recommendation were made without a quorum present (key SME's from the business stakeholders, USDA, DOI and FS).

Core Team

Core Team Member	Representing
Kolleen Beesley	IIOG Program Manager - FS
Dan Glover	<i>Project Lead</i> - ICAM Specialist – FS CIO
Stuart Ott	Service Delivery Division – DOI OCIO
Pam Weber	Director ICAM Division – USDA OCIO
Adam Zeiment	Chief Architect / IT Specialist - USDA OCIO
Lani Williams	Fire Applications Business Specialist / Business Representative - FS FAM
Clint Swett	Acting ACIO, International Technology Services (USDA / OCIO)
John Young	Windows Admin. Team Lead - International Technology Services (USDA / OCIO)
Lou Eichenbaum	Chief Information Security Officer – BLM
Eileen Richey	IIOG Project Manager - FS

Additional Team Participants

Participant Name	Representing
Laura Hill	FAM IT Strategic Planner - FS
Chuck Womack	National Coordination Center Assistant Manager - BLM
Susie Stingley-Russell	National Coordination Center Manager - FS
Pat Price	Project Manager - Information Assurance, FICAM, Strong Authentication - DOI
Jim Douglas	DOI – Director, Office of Wildland Fire Coordination – IIOG Chair
Sandy Watts	Assistant Director, Enterprise Business Solution Services – FS CIO
Doug Nash	Chief Information Officer - FS CIO
Brad Smith	Branch Chief, Enterprise Content Management/eDiscovery – FS CIO
Dan Boss	IT Specialist - International Technology Services (USDA / OCIO)
Tim Lee	International Technology Services (USDA / OCIO - ITS)
Chris Moyer	National Service First Program Manager (FS & BLM)
Laurence Lee	Solution Architect Program Assessment and Evaluation / Service Delivery – DOI OCIO

3. Approach

A high-level description of the process used to identify and rank alternatives included:

- Business leads collaborated with customers/stakeholders to re-validate the stated business needs. A few new business needs were identified for consideration. A full interagency quorum of project team SMEs from the business (FAM, Service First, etc.), as well as technical experts from the USDA, DOI and FS were present at each meeting before any decision work toward recommendations was completed.
- A discussion of each business need and potential solution was conducted by the project team. The business needs naturally fell into three general categories, each best addressed by different technical approaches.
 - **Category 1** - The need for USDA and DOI government employees to be able to securely collaborate and work together, regardless of their location.
 - This subset of needs was identified as best solved by some form of credential sharing. Options 1 and 2 in the analysis address these needs.
 - **Category 2** - The need for both/either Department to collaborate and interact with non-Federal public/state/private entities.
 - This subset of needs was best addressed by cloud environment (options 3 and 4) to facilitate use by non-Federal cooperators.
 - **Category 3** – Items outside the scope of this project. Newly identified or refined business needs were solved using this methodology while others were determined to be outside the scope of the project.

The interagency project team discussed and analyzed the broad range of options and combined them into four possible alternatives that best meet the majority of key business needs.

The project team compared benefits/value (enduring business value) versus:

- Cost to implement and maintain.
- Risk of project success/failure.
- Potential political challenges.
- Relative implementation costs.
- Timeframe to completion.

4. Alternatives

Alternative 1 - One AD/Net w/External Public Cloud

Description – Alternative 1 joins the USDA and DOI network into one shared environment (both network and Active Directory). Non-Federal Cooperators are facilitated by the use of an externally hosted cloud environment.

Political Concerns

- It is unlikely that sharing one Active Directory (AD) Forest between DOI and USDA will be acceptable to Chief Information Security Officers (CISO) of the respective departments. To implement this option potentially jeopardizes their ability to control security boundaries extending outside their department.
- Appropriation and fiscal concerns become complicated. Assigning benefit per agency becomes difficult to reconcile with investment per agency.
- Trusted Internet Connection (TIC) compliancy needs to be a coordinated effort between departments and fully integrate the business requirements into a standardized methodology. Therefore the one shared external cloud provider chosen must meet FEDRAMP requirements. This will require acceptance by OMB/NIST.

Quick Wins – Implementation of an external cloud will quickly facilitate hosting shared email and file sharing available to Fed Employees and Non-Federal cooperators. However there is a risk that implementing this quick win could leave the customers without a comprehensive solution which meets the majority of the business needs.

Timeframe to Completion – The team estimates four years from approval with available resources.

Value Analysis (End User Business Needs) – See Appendix A – Value Analysis.

Risks – See Appendix B - Risk Analysis

Level of Effort / Resources Needed (People, time, money) - The specific resources required to implement this alternative will be identified during full project plan development. Full project plan development should only occur if this alternative is selected as management's preference for implementation. However, in order to rank alternatives, the project team developed a relative cost rating for each alternative. This information is available in Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed.

Summary – This is the second preferred alternative. The team feels that this alternative best meets the business needs, but is far more complex to implement than Alternative 2.

Alternative 2 - DOI / USDA Inter-forest Trust w/External Public Cloud

(Recommended Alternative)

Description – Alternative 2 creates a trusted environment between DOI and USDA Active Directory (AD). Non-Federal Cooperators are facilitated by the use of an externally hosted cloud environment.

Political Concerns

- There is increased risk in inter-forest trust between USDA and DOI associated with reciprocally trusting credentials. However, the Memorandum of Understanding (MOU) for Interagency Recognition of Security Controls and Credentials between the Department of Agriculture and Department of the Interior [Interagency Recognition of Security Controls and Credentials MOU](#) signed in October of 2010 states that we are subject to the same body of law and requirements with respect to the security, management and protection of Information Technology (IT) resources. Therefore the signatories agree reciprocally accept each department's security controls and credentials for the express purposes of sharing resources and services. This MOU was put in place to facilitate this project.
- Trusted Internet Connection (TIC) compliancy needs to be a coordinated effort between departments in order to fully integrate the business requirements into a standardized methodology. Therefore the single shared external cloud provider must meet FEDRAMP requirements. This requires acceptance by OMB/NIST.

Quick Wins – Implementation of an external cloud quickly facilitates hosting shared email and file sharing available to Federal Employees and Non-Federal cooperators.

Timeframe to Completion – The team estimates one year from approval with available resources.

Value Analysis (End User Business Needs) – See Appendix A – Value Analysis.

Risks – See Appendix B - Risk Analysis.

Level of Effort / Resources Needed (People, time, money) - The specific resources required to implement this alternative will be identified during full project plan development. Full project plan development should only occur if this alternative is selected as management's preference for implementation. However, in order to rank alternatives, the project team developed a relative cost rating for each alternative. This information is available in Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed.

Summary – Recommended alternative. The team feels that this alternative is the most viable to implement and maintain, offers the shortest timeframe to implementation and best meets the business needs of the customers.

Alternative 3 - One AD/NET w/Internal Cloud Hosted by One Agency Only

Description – Alternative 3 joins the USDA and DOI network into one shared environment (both network and AD). File sharing amongst USDA and DOI partners is facilitated by use of an internally hosted cloud (hosted by one agency). Non-Federal Cooperator access is not facilitated until HSPD-12 PIV credential direction for non-federal entities is resolved.

Political Concerns

- It is unlikely that sharing one AD Forest between DOI and USDA is acceptable to Chief Information Security Officers (CISO) of the respective departments. To implement this option potentially jeopardizes their ability to control security boundaries extending outside their department.
- Appropriation and fiscal concerns become complicated. Assigning benefit per agency becomes difficult to reconcile with investment per agency.
- Internal cloud hosting by one agency could provide fiscal challenges including who pays for, manages and secures the environment.
- Non-Federal partner sharing is not facilitated. There continues to be work-around methods that will likely pose potentially new, unknown security vulnerabilities.

Quick Wins – None known.

Timeframe to Completion – The team estimates four years from approval with available resources.

Value Analysis (End User Business Needs) – See Appendix A – Value Analysis.

Risks – See Appendix B - Risk Analysis.

Level of Effort / Resources Needed (People, time, money) - The specific resources required to implement this alternative will be identified during full project plan development. Full project plan development should only occur if this alternative is selected as management's preference for implementation. However, in order to rank alternatives, the project team developed a relative cost rating for each alternative. This information is available in Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed.

Summary - The team feels that this alternative is less than a complete solution in that it minimally meets the business needs. The team does not recommend implementation of this alternative.

Alternative 4 - DOI / USDA Inter-Forest Trust w/Internal Cloud Hosted by One Agency Only

Description – Alternative 4 creates a trusted environment between DOI and USDA Active Directory (AD). File sharing amongst USDA and DOI partners is facilitated by use of an internally hosted cloud (hosted by one agency). Non-Federal Cooperator access is not facilitated until HSPD-12 PIV credential direction for non-federal entities is resolved.

Political Concerns

- Appropriation and fiscal concerns become complicated. Assigning benefit per agency becomes difficult to reconcile with investment per agency.
- There is increased risk in inter-forest trust between USDA and DOI associated with reciprocally trusting credentials. However, the Memorandum of Understanding (MOU) for Interagency Recognition of Security Controls and Credentials between the Department of Agriculture and Department of the Interior [Interagency Recognition of Security Controls and Credentials MOU](#) signed in October of 2010 states that we are subject to the same body of law and requirements in respect to the security, management and protection of Information Technology (IT) resources. Therefore the signatories have agreed to reciprocally accept each department's security controls and credentials for the express purposes of sharing resources and services. This MOU was put in place to facilitate this project.
- Internal cloud hosting by one agency could provide fiscal challenges including who pays for, manages and secures the environment.
- Non-Federal partner sharing is not facilitated. There will continue to be work arounds identified that pose potentially new, unknown security vulnerabilities.

Quick Wins – None known.

Timeframe to Completion – The team estimates one year from approval with available resources.

Value Analysis (End User Business Needs) – See Appendix A – Value Analysis.

Risks – See Appendix B - Risk Analysis.

Level of Effort / Resources Needed (People, time, money) - The specific resources required to implement this alternative will be identified during full project plan development. Full project plan development should only occur if this alternative is selected as management's preference for implementation. However, in order to rank alternatives, the project team developed a relative cost rating for each alternative. This information is available in Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed.

Summary - The team feels that this alternative is less than a complete solution because it minimally meets the business needs. The team does not recommend implementation of this alternative.

5. Quick Wins

Regardless of the alternative selected, suspension of the USDA limitation on email access via the internet is a quick win. This action would facilitate access to email by employees using either FS or DOI computer/network.

6. Next Steps / Additional Recommended Actions

- After alternative selection and direction to implement by management; the project team needs to develop a full project plan. Time necessary to develop the plan will be dependent upon the alternative selected.
- In order to facilitate interagency supervision, timesheets, travel, and performance rating related documents need to be approved by either DOI or USDA agency supervisors for employees working under their direction regardless of agency employer. **The Project Team recommends that Management appoint a Tiger Team to resolve this situation.** Recommended team members would include business representatives such as, a member of this project team, and expertise from Human Capital Management (HCM) for resolution.
- The ability for non-Federal cooperators to log-on to either USDA or DOI network without PIV card is not resolved and is outside the scope of this project. Therefore the external cloud recommendation is the viable method with the shortest time to implement to resolve this situation.
- Ability to log on to **more than one computer** simultaneously once PIV cards are required is outside the scope of this project. This is particularly challenging when PIV is required for VPN.
- Ensuring **compatibility of software versions** between DOI and USDA is necessary to support some customers. This is a governance issue and outside the scope of this project and may require a follow-on project once an alternative is implemented.
- **Helpdesk** support does not cross well between USDA and DOI and a project will be necessary to enhance this capability.

Appendix A – Value Analysis

Full details of team analysis work is contained in Attachment 1 – Detailed Analysis Calculations and References

Each alternative was rated against value factors as in the charts described below:

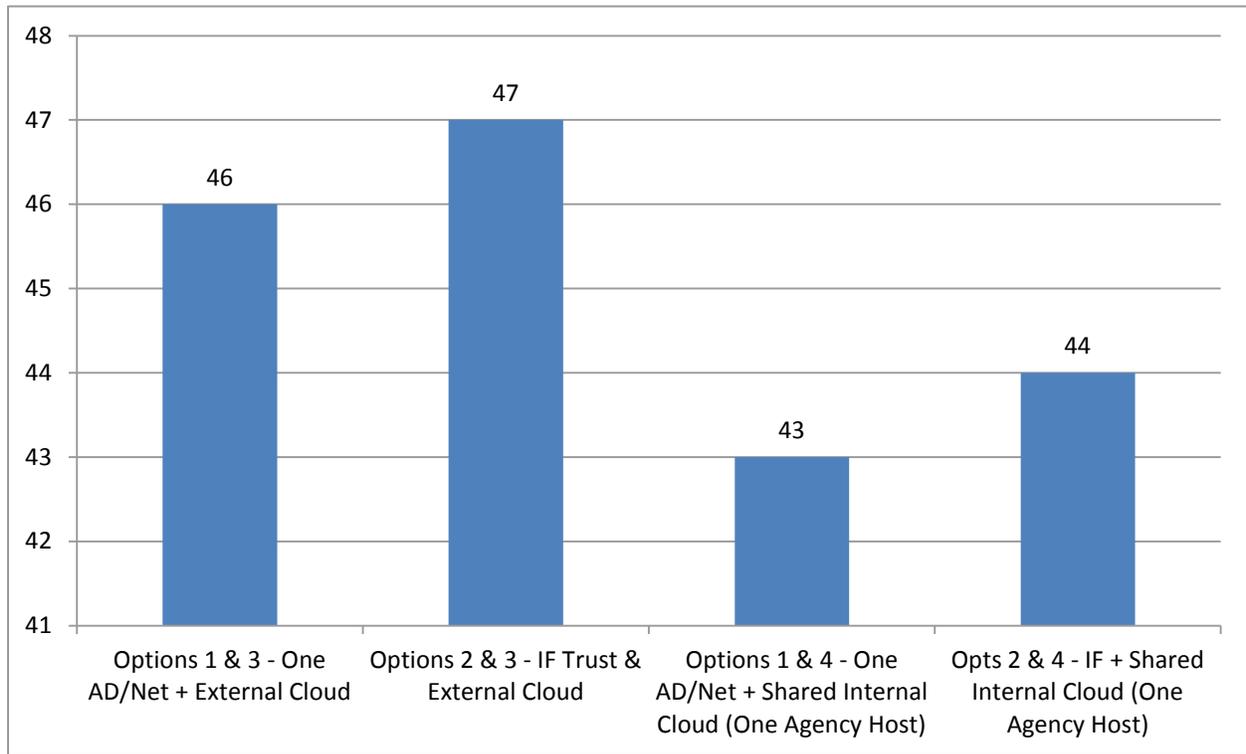
Major value factors (from which the value hierarchy is developed) include:

- **End User Value:** benefits to customers/clients. For example, convenient access, product enhancement
- **Operational Value:** better operations and lowering barriers to future initiatives. For example, improved infrastructure
- **Strategic/Political Value:** contributions to strategic initiatives and fulfilling the mission of the organization.
- **Social Value:** benefits to society as a whole, e.g. reducing CO₂ emissions.

Value Metric		Alt 1 Options 1 & 3 - One AD/Net + External Cloud	Alt 2 Options 2 & 3 - IF Trust & External Cloud	Alt 3 Options 1 & 4 - One AD/Net + Shared Internal Cloud (One Agency Host)	Alt 4 Opts 2 & 4 - IF + Shared Internal Cloud (One Agency Host)
End User	Intuitive, Good experience	Robust	Robust	Average	Average
	Access to Home Agency Apps from Away	Robust	Robust	Robust	Robust
	Ease of use, Interface	Robust	Robust	Robust	Robust
	Simultaneous Interoperability with Other Fed Systems (DOI/USDA)	Robust	Robust	Robust	Robust
	Required security/encryption (where needed)	Robust	Robust	Robust	Robust
	Operational functionality (Shared Files / Printers / Etc)	Robust	Good	Robust	Good
	Minimal User Impacts (Operational Maintenance Activity) - Migration	Limited	Good	Limited	Good
	Minimal User Impacts (Operational Maintenance Activity) - Operations	Average	Average	Good	Good
	Support (Help desk) - Communication Complexity to Resolving Issues	Adequate	Adequate	Adequate	Adequate
	User Impact - Needed Training	Robust	Good	Good	Average
User Impact - Consistency In Operations between USDA/DOI Employee Experience	Robust	Robust	Good	Good	
Foundational/ Operational	Single Desktop / Individual Work - Dual eMail Access	Robust	Robust	Robust	Robust
	Ease of maintenance	Average	Good	Average	Average
	Availability of personnel with required skill sets	Adequate	Good	Average	Average
	Documented operating procedures and system operations	Average	Average	Adequate	Average
	Ease of acquiring new / replacement equipment	Average	Good	Adequate	Average
	Ease of installation (e.g., configuration, provisioning, testing)	Average	Good	Average	Average
	Adaptability (e.g., emergency response)	Good	Good	Average	Average
	Shared Inboxes for Incident Support (Fed and Non-Fed Access)	Average	Good	Good	Good
	Scalability	Average	Robust	Average	Average
Ease of integration with rest of IT infrastructure	Robust	Average	Average	Average	
Strategic/Political	Compliance with Executive Initiatives	Good	Average	Good	Average
	Compliance with Departmental Secretarial Orders (3309, etc)	Good	Average	Good	Average
	Compliance with Federal (OMB, E-Gov) Strategic Plans	Good	Good	Average	Average
	Address external NGO stakeholders	Adequate	Good	Adequate	Adequate
	Address internal bureau/agency stakeholders	Average	Good	Average	Average
	Address Congressional Concerns	Average	Adequate	Adequate	Adequate
	Address other government agencies access needs (States, etc)	Average	Average	Adequate	Adequate
	Address internal oversight and regulation entities	Good	Average	Good	Average
Social	Public confidence in system data	Average	Average	Average	Average
	Public confidence in disaster recovery	Average	Average	Adequate	Adequate
	Efficiency of acquisition and operations	Average	Good	Adequate	Adequate
	Accountability	Good	Average	Average	Average

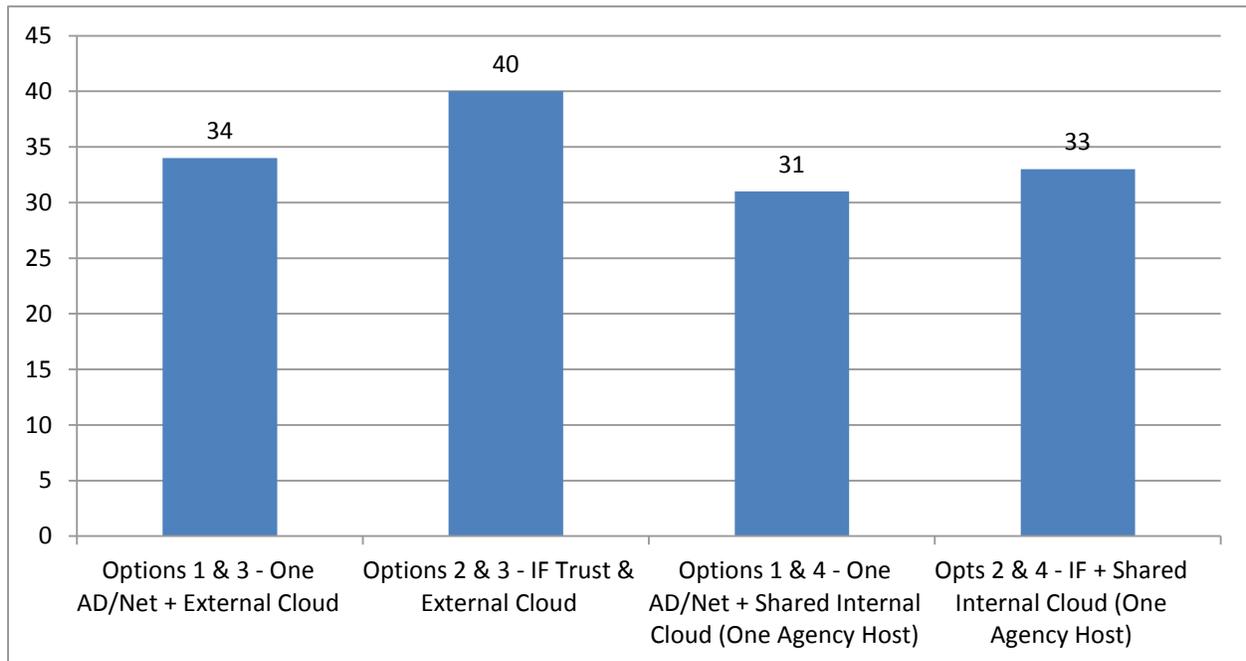
End User

Alternative 2 ranked highest, followed by Alternative 1, 4 and 3 respectively.



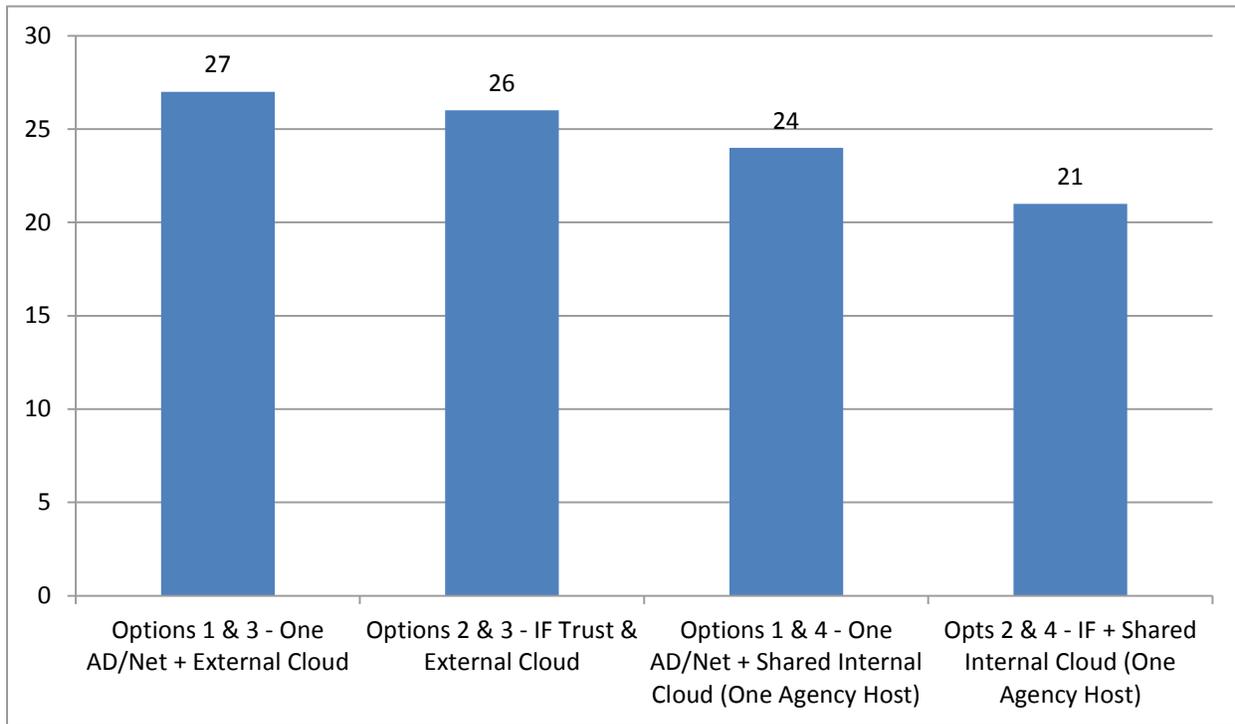
Foundational / Operational

Alternative 2 ranked highest, followed by Alternative 1, 4 and 3 respectively.



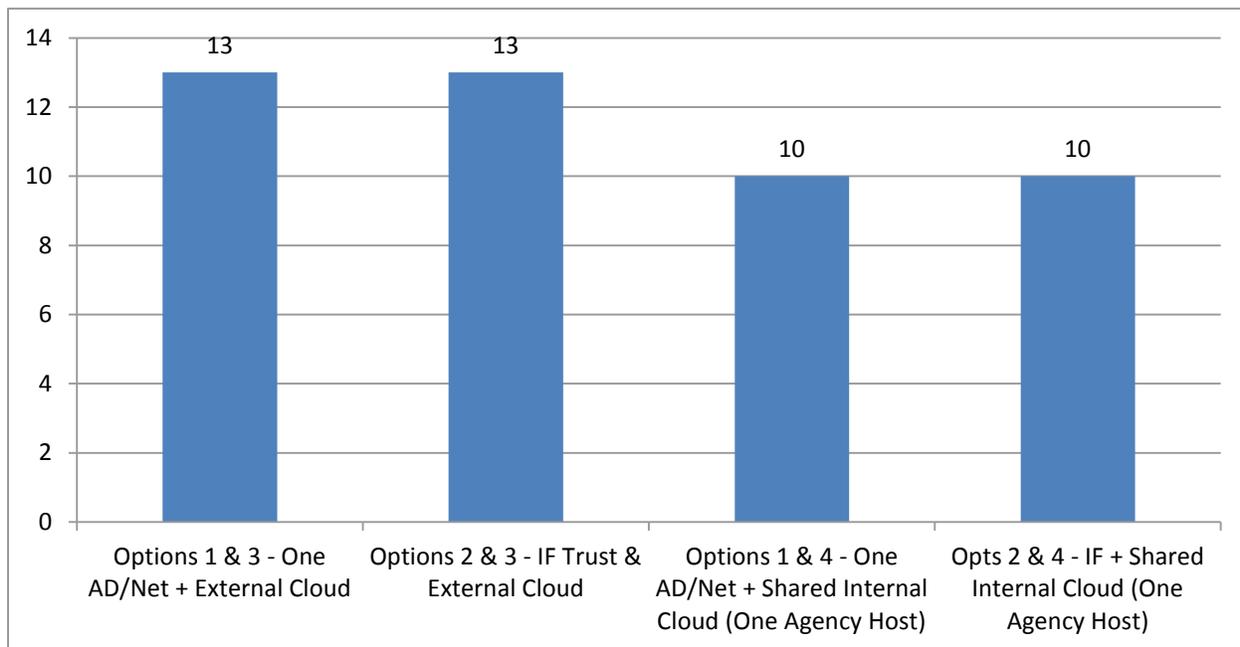
Strategic / Political

Alternative 1 ranked highest followed by Alternative 2, 3, and 4, respectively.



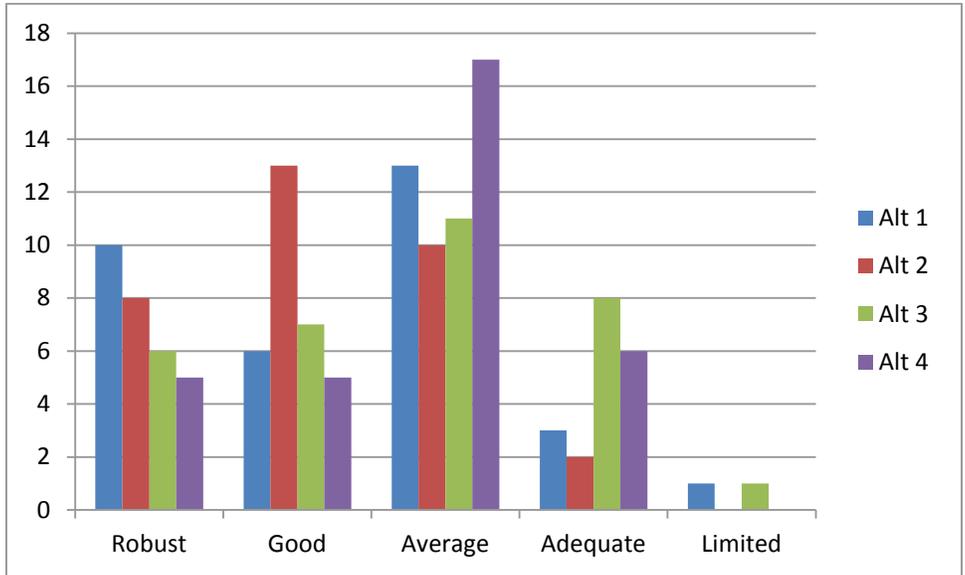
Social

Alternative 1 and 2 scored equally followed by Alternative 3 and 4 which also scored equally.



When all Alternatives were ranked according to all value categories collectively, only Alternative 4 had a predominant advantage in the Average category and Alternative 2 maintained a distinct advantage in the Good Category.

Summary of Overall Value



In terms of overall Value, Alternative 2 had the highest defined value with 126 points, followed by Alternative 1 with 120 points and Alternatives 3 and 4 which both scored 108 points.

Alternative 1 Total Value Score	120
Alternative 2 Total Value Score	126
Alternative 3 Total Value Score	108
Alternative 4 Total Value Score	108

Appendix B - Risk Analysis

The team measured each alternative in terms of risk as defined by OMB in their Circular A-11.

1. **Schedule:** Risk associated with schedule slippages, either from lack of internal controls or those associated with late delivery by vendors, resulting in missed milestones.
2. **Initial Costs:** Risk associated with “cost creep” or miscalculation of initial costs that result in an inaccurate baseline against which to estimate and compare future costs.
3. **Life Cycle Costs:** Risk associated with misestimating life-cycle costs and exceeding forecasts; reliance on a small number of vendors without sufficient cost controls.
4. **Technical Obsolescence:** Risk associated with technology that becomes obsolete before the completion of the life cycle and cannot provide the planned and desired functionality.
5. **Feasibility:** Risk that the proposed alternative fails to result in the desired technological outcomes; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
6. **Reliability of Systems:** Risk associated with vulnerability/integrity of systems.
7. **Dependencies and Interoperability between this Investment and Others:** Risk associated with interoperability between other investments; risk that interoperable systems will not achieve desired outcomes; risk of increased vulnerabilities between systems.
8. **Surety (asset protection) Considerations:** Risk associated with the loss/misuse of data or information; risk of technical problems/failures with applications; risk associated with the security/vulnerability of systems.
9. **Risk of Creating a Monopoly for Future Procurements:** Risk associated with choosing an investment that depends on other technologies or applications that require future procurements to be from a particular vendor or supplier.
10. **Capability of Agency to Manage the Investment:** Risk of financial management of investment, poor operational and technical controls, or reliance on vendors without appropriate cost, technical and operational controls; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
11. **Overall Risk of Project Failure:** Risk that the project/investment will not result in the desired outcomes.
12. **Project Resources/Financial:** Risk associated with "cost creep," or miscalculation of life-cycle costs; reliance on a small number of vendors without cost controls, or (poor) acquisition planning.
13. **Technical/Technology:** Risk associated with immaturity of commercially available technology and reliance on a small number of vendors; risk of technical problems/failures with applications and their ability to provide planned and desired technical functionality.
14. **Business/Operational:** Risk associated with business goals; risk that the proposed alternative fails to result in process efficiencies and streamlining; risk that business goals of the program or initiative will not be achieved; risk that the investment will not achieve operational goals; risk that the program effectiveness targeted by the project will not be achieved.

15. **Organizational and Change Management:** Risk associated with organizational, agency, or Government-wide cultural resistance to change and standardization; risk associated with bypassing or lack of use or improper use or adherence to new systems and processes because of organizational structure and culture; inadequate training planning.
16. **Data/information:** Risk associated with the loss or misuse of data or information, risk of compromise of citizen or corporate privacy information; risk of increased burdens on citizens and businesses because of data collection requirements if the associated business processes or the project (being described in the Exhibit 300) requires access to data from other sources (federal, state, and/or local agencies).
17. **Security:** Risk associated with the security/vulnerability of systems, web sites, information and networks; risk of intrusions and connectivity to other (vulnerable) systems; risk associated with the evolution of credible threats; risk associated with the misuse (criminal/fraudulent) of information; must include level of risk (high, medium, basic) and what aspect of security determines the level of risk (e.g., need for confidentiality of information associated with the project/system, availability of the information or system, or reliability of the information or system).
18. **Strategic:** Risk associated with strategic/government-wide goals (i.e., President's Management Agenda and e-Gov initiative goals); risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them.
19. **Privacy:** Risk associated with the vulnerability of information collected on individuals or risk of vulnerability of proprietary information on businesses.

The following table illustrates how each Alternative was ranked using a standard risk table (probability x magnitude = impact):

Probability	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Magnitude				

OMB Risk Areas		Probability				Magnitude				Impact			
		Alt 1 Options 1 & 3 - One AD/Net + External Cloud	Alt 2 Options 2 & 3 - IF Trust & External Cloud	Alt 3 Options 1 & 4 - One AD/Net + Shared Internal Cloud (One Agency Host)	Alt 4 Opts 2 & 4 - IF + Shared Internal Cloud (One Agency Host)	Alt 1 Options 1 & 3 - One AD/Net + External Cloud	Alt 2 Options 2 & 3 - IF Trust & External Cloud	Alt 3 Options 1 & 4 - One AD/Net + Shared Internal Cloud (One Agency Host)	Alt 4 Opts 2 & 4 - IF + Shared Internal Cloud (One Agency Host)	Alt 1 Options 1 & 3 - One AD/Net + External Cloud	Alt 2 Options 2 & 3 - IF Trust & External Cloud	Alt 3 Options 1 & 4 - One AD/Net + Shared Internal Cloud (One Agency Host)	Alt 4 Opts 2 & 4 - IF + Shared Internal Cloud (One Agency Host)
1	Schedule	3	3	3	3	4	3	4	3	12	9	12	9
2	Initial costs	3	3	3	4	4	2	4	3	12	6	12	12
3	Life-cycle costs	4	4	3	4	4	3	4	3	16	12	12	12
4	Technical obsolescence	3	3	3	3	3	2	3	2	9	6	9	6
5	Feasibility	2	2	3	3	4	3	4	3	8	6	12	9
6	Reliability of systems	3	3	3	3	4	3	4	3	12	9	12	9
7	Dependencies and interoperability between this investment and others	4	4	3	4	3	2	3	2	12	8	9	8
8	Surety (asset protection) considerations	3	3	3	3	3	3	3	3	9	9	9	9
9	Risk of creating a monopoly for future	2	2	2	2	3	2	3	2	6	4	6	4
10	Capability of agency to manage the investment	3	3	3	3	4	3	4	3	12	9	12	9
11	Overall risk of project	4	3	4	3	4	3	4	3	16	9	16	9
12	Project resources/financial	4	3	4	3	3	3	3	3	12	9	12	9
13	Technical/technology	2	2	2	2	4	3	4	3	8	6	8	6
14	Business/operational	4	4	4	4	4	3	4	3	16	12	16	12
15	Organizational and change	3	3	4	4	3	3	3	3	9	9	12	12
16	Data/information	4	3	4	3	4	4	4	4	16	12	16	12
17	Security	4	4	4	4	4	4	4	4	16	16	16	16
18	Strategic	3	3	4	4	3	3	3	3	9	9	12	12
19	Privacy	3	3	3	3	4	4	4	4	12	12	12	12

Agg. Score 11.68 9.05 11.84 9.84

Overall Rating for assessing risk resulted in Alternative 2 as a slightly lower risk than Alternative 4 as well as Alternatives 1 and 3 which scored equally.

Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed (People, Time, Money)

While the team was not able to analyze costs in terms of actual dollars spent on each major component involved (i.e., Telecommunications, servers, software, licensing, contractual costs, etc.), the team scored costs in terms of capital outlays, cost avoidance and benefits as follows:

Score	Capital Outlay	Cost Avoidance and Benefits
1	Negligible	Little or no impact to current IT funding levels (< 5%)
2	Minor	Small increase to current IT Funding levels (< =10%)
3	Moderate	Noticeable increase to current IT funding levels (<=25%)
4	Significant	Major increase to current IT funding levels (<=40%)
5	Cost Prohibitive	Substantial increase to current IT Funding levels (<=60%)

Will this Alternative Cost More or Less in Out-Years than in Today's Steady State?

Scores: Negligible = 1, Minor = 2, Moderate = 3, Significant = 4, Cost Prohibitive = 5

Key Cost Component	Alt 1 Options 1 & 3 - One AD/Net + External Cloud	Alt 2 Options 2 & 3 - IF Trust & External Cloud	Alt 3 Options 1 & 4 - One AD/Net + Shared Internal Cloud (One Agency Host)	Alt 4 Opts 2 & 4 - IF + Shared Internal Cloud (One Agency Host)	Remarks
Implementation Costs					
Circuit & Network	4	3	4	4	
Directory/Account Service	4	2	4	2	
O&M Requirements*					
Circuit & Network	3	2	3	3	* Demand and traffic expected to grow significantly once implemented. This could drive costs up as additional services are requested and bandwidth requirements increase.
Directory/Account Service	1	3	1	3	
Potential Cost Avoidance (Benefit)					
Field Workaround Reduction	1	2	2	2	Economies of Scale create a significant cost avoidance.
Reduce Internal Security Risks	1	1	2	2	Field work-arounds create unintended security risks.
Reduce External Security Risks	1	1	2	2	Field work-arounds create unintended security risks.
Policy / Litigation Hold Mitigation	1	1	1	1	
Service First - Facilities Savings	1	2	1	2	
Reduction Hardware Costs	1	1	1	1	Printers, network equipment, desktop/laptop,
Reduction Software Licensing	1	1	1	1	
Reduction in Contracting	1	1	1	1	
Service First Implementation	1	1	1	1	
Implementation	4.00	2.50	4.00	3.00	Average Cost Impact to Implement
O&M	2.00	2.50	2.00	3.00	Average Cost Impact to Operate and Maintain
Cost Avoidance Average	1.00	1.22	1.33	1.44	Average Cost Avoidance

Appendix D - Summary of USDA / DOI Risk and Value Assessment for Solution Alternatives

Alternatives 3 & 4 are less than complete solutions (minimally meet Business Needs)

- The Value Scores as calculated in Appendix A – Value Analysis combined with the Average Value of the Scores for each of the four separate Major Value Factors are provided in the table below.
- Each of the averaged Major Value Factors was then combined to provide an overall Average Value Score for each Alternative.
- Risk Percentages were derived from the Risk Table Impacts shown in Appendix B - Risk Analysis and Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed.
- Using Implementation Costs (Investment) as the majority of the expenditures, Relative Costs were weighted by the Risk Score Percentage and added back into the value to derive the Risk Adjusted Relative Cost %.
- The comparison of the Average Value Scores and Risk Scores from Appendix B - Risk Analysis shows the Relative Cost Scores clearly define Alternative 2 as the Preferred Alternative.

Summary of USDA / DOI Risk and Value Assessment for Access Authentication Solution Alternatives

Alternatives 3 & 4 are less than complete solutions because they do not facilitate non-Federal partner sharing/participation (minimally meet Business Needs)

	Alt 1	Alt 2	Alt 3	Alt 4	
	Options 1 & 3 - One AD/Net + External Cloud	Options 2 & 3 - IF Trust & External Cloud	Options 1 & 4 - One AD/Net + Shared Internal Cloud (One Agency Host)	Opts 2 & 4 - IF + Shared Internal Cloud (One Agency Host)	
Average Value Scores	3.55	3.69	3.13	3.11	
End User Needs Average Rating	4.18	4.27	3.91	4.00	
Foundational / Operational - Average Rating	3.40	4.00	3.10	3.30	
Strategic / Political - Average Rating	3.38	3.25	3.00	2.63	
Social - Average Rating	3.25	3.25	2.50	2.50	
Risk Scores	11.68	9.05	11.84	9.84	
Relative Costs					
(Investment) Implementation	4.00	2.50	4.00	3.00	Ave. Cost Impact to Implement
O&M	2.00	2.50	2.00	3.00	Ave. Cost Impact to Operate and Maintain
Cost Avoidance (Benefit) Average	1.00	1.22	1.33	1.44	Ave. Cost Avoidance
Risk Adjusted Relative Costs %	4.47	2.73	4.47	3.30	
		1st Choice Best	2nd Choice		

Attachment 1 – Detailed Analysis Calculations and References

The [Access Authentication Detailed Analysis Calculations and References Spreadsheet](http://www.IIOG.gov/documents/aanalysis.xls) is available by clicking on this [link to http://www.IIOG.gov/documents/aanalysis.xls](#). It contains additional the details associated with the tables contained in Appendix A – Value Analysis, Appendix B - Risk Analysis, Appendix C – Cost Analysis / Relative Cost Rating – Level of Effort / Resources Needed and Appendix D - Summary of USDA / DOI Risk and Value Assessment for Solution Alternatives.