



Information Sharing Working Group

Federated Governance of Information Sharing Within the Extended Enterprise

January 15, 2008

Principle authors:

Bryan Aucoin, Alanthus Associates
Jarl S. Magnusson, Det Norske Veritas

Association for Enterprise Integration
2111 Wilson Boulevard, Suite 400
Arlington, Virginia 22201



2111 Wilson Boulevard
Suite 400
Arlington, Virginia 22201

Ms. Debra M. Filippi
Information Sharing Executive
DoD CIO
1851 S Bell St
Arlington, VA 22202

January 15, 2008

Dear Ms. Filippi

I am pleased to submit to you this product of the AFEI Information Sharing Working Group. This white paper, *Federated Governance of Information Sharing within the Extended Enterprise*, is intended to provide concepts and approaches for the governance of information sharing in large federated environments, and to provide recommendations and insight regarding Information Sharing Governance.

I wish to thank all of the contributors to this effort including the principle authors, Bryan Aucoin, formerly of Enterra Solutions and now a principle in Alanthus Associates, and Mr. Jarl Magnusson of Det Norske Veritas. I am also grateful to the support lent to the working group by Mr. Paul Grant of your office.

The Association and its members are pleased to support the efforts of the DoD CIO and the Information Sharing Executive, and look forward to continuing to develop the concepts, ideas and recommendations contained in the document.

Respectfully,

David E. Chesebrough, P.E.
President



Acknowledgements

AFEI wishes to acknowledge the contributions of its member companies in making the resources available to complete this project.

In particular AFEI thanks **Enterra Solutions** for making Mr. Bryan Aucoin available to both co-chair the Information Assurance Working Group and to be a principle author of this white paper. AFEI also recognizes the contributions of other Enterra Solutions staff, including Mr. Bill Tucker. Bryan was instrumental in bringing the EPA, Department of the Interior and OMB into the project.

AFEI also wishes to thank **Det Norske Veritas** for providing Mr. Jarl Magnusson as both co-chair of the Information Sharing Working Group and principle author of this white paper. Mr. Magnusson was instrumental in getting the perspective of the Swedish Ministry of Defense.

About Enterra Solutions

Enterra Solutions is the leader in Enterprise Resilience Management™ - a new enterprise architecture that enables public and private-sector organizations to respond to the stressors that result from globalization, rapid technological change, terrorism, natural disasters, and other 21st century challenges. Enterra's proprietary Enterprise Resilience Management Solution™ (ERMS™) consists of a best-practices methodology and technology solution that automates rules sets and integrates security, compliance and business process optimization into a single function - to generate a powerful platform that transforms the organization into a Resilient Enterprise™. Visit them at <http://www.enterrasolutions.com>.

About Det Norske Veritas

Established in 1864, Det Norske Veritas (DNV) is an independent foundation with the objective of safeguarding life, property and the environment and is a leading international provider of services for managing risk. The Information Quality Management (IQM) group of DNV is aligned with existing DNV businesses. DNV IQM delivers services to help customers safeguard their information assets, thus supporting DNV's objective to "safeguard life, property and the environment". Visit them at http://www.dnv.us/it_telecom/iqm.



Information Sharing Working Group White Paper

**Federated Governance of Information Sharing Within the
Extended Enterprise**

Submitted to

Ms. Debra M. Filippi
Information Sharing Executive
DoD CIO
1851 S Bell St
CM #3
Arlington, VA 22202

January 15, 2008

Abstract

The purpose of this document is to provide concepts and approaches for the governance of information sharing in large federated environments, and to provide recommendations and insight regarding Information Sharing Governance. There is no “one-size fits all” style of governance within federated environments. The style of governance must be tailored for the state or phase of evolution of a given federation as it forms and self-organizes. The end-game of the evolution of a federation formed for information sharing is information stewardship. Information stewardship is a best practice based upon empirical assessment of Information Technology (IT) governance and common practice within the public and private sectors.

This paper defines the concept of a “meta-governor”. The role of a meta-governor is to guide federations through their evolutionary processes toward information stewardship. The paper provides guidance, in the form of checklists, for meta-governance, federations, and information stewards. These checklists are at a high level. However, they provide direction for follow-on work by the AFEI in establishing detailed implementation guidance within each of these areas.

The heart of this work is represented by Table 4.1 on page 38, which offers a synopsis of actions that should be taken by self-forming federations (including communities of interest and practice) with respect to information sharing governance.



Key Contributors and Advisors:

US Government:

Paul Grant	DoD ASD(NII)/DoD CIO
Debra Filippi	Information Sharing Executive, DoD
Suzanne Acar	US Dept. of Interior, Senior Information Architect
Mary McCaffery	US Environmental Protection Agency, Special Advisor to the Chief Information Officer
Kshemendra Paul	Acting Chief Architect, OMB

Swedish Government:

Peder Blomqvist	Swedish Defense HQ CIO Strategy
-----------------	---------------------------------

Private Sector:

Michael Daconta	Chief, Enterprise Data Management, Oberon Associates, Inc.
William Tucker	Senior Business Analyst, Enterra Solutions
Jim Cisneros	The Boeing Corporation, Integrated Defense Systems
Steve DeAngelis	CEO, Enterra Solutions



Table of Contents

Executive Summary vi

Foreword viii

1. Introduction..... 1

 1.1. Purpose 1

 1.2. Scope..... 1

 1.3. Structure of This Paper..... 2

2. Statement of Need (Current State)..... 3

 2.1. An Imperative to Continue Progress..... 3

 2.2. Governance Needs..... 4

 2.2.1. Governance and Culture 5

 2.2.2. Governance and Policy:..... 8

 2.2.3. Governance and Resources 9

 2.2.4. Governance and Technology..... 10

3. Vision for the Future 12

 3.1. A Framework for Governance 12

 3.1.1. The Evolution of Concepts and Their Governance..... 13

 3.1.2. Best Practices for Information Technology Governance 16

 3.2. Information Sharing Principles..... 18

 3.2.1. Information is a valuable asset 18

 3.2.2. Other principles and precepts 20

 3.3. Target State Governance 21

 3.3.1. Using Governance to Effect Culture 23

 3.3.2. Using Governance to Effect Policy 26

 3.3.3. Using Governance to Effect Economics and Resources 27

 3.3.4. Using Governance to Effect Technology 29

 3.3.5. Data Architecture and Data Sharing Architecture:..... 30

 3.3.6. Identity Management and Policy/Attribute –Based Access Management 32

4. Transition – The Checklist..... 34

 4.1. For The Extended Enterprise 34

 4.1.1. Phase 0 – General: 34

 4.1.2. Phase I – Instantiation: 35

 4.1.3. Phases II and III – Aggregation, Codification and Reconciliation 35

 4.1.4. Phase IV - Assimilation 36

 4.2. For Federations, Communities of Interest, Communities of Practice 38

 4.3. For Information Stewards: 40

5. Recommendations for Follow-On Action:..... 41

Appendix A - References 43

Appendix B - Definitions..... 44



Executive Summary

In May, 2007, the Department of Defense (DoD) issued an Information Sharing Strategy that provides a common vision to synchronize information throughout the Department. The strategy defines information sharing as: *“Making information available to participants (people, processes, or systems).”* Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.

This Strategy will guide the exchange of information within the DoD and with Federal, state, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector (external partners). The DoD and these external partners are referred to at the *Extended Enterprise*.

The DoD will develop an Information Sharing Strategic Implementation Plan as a companion document. This Plan will provide integrated guidance to synchronize the many information sharing activities, initiatives and investments supported by the DoD, including both internally and externally sponsored efforts. The Plan will provide descriptions of the specific actions, roles, responsibilities, milestones, metrics, and priorities for execution of information sharing activities.

DoD ASD(NII)/DoD CIO requested the Association for Enterprise Integration (AFEI) Information Sharing Working Group (ISWG) to bring together senior leadership from the public, private and academic sectors and to produce recommendations and a check list for implementing governance within large, federated environments. In line with DoD Information Sharing Strategy, the ISWG focused on governance concepts and approaches that are:

- Self-forming, self-organizing and self-regulating;
- Required to support the establishment and maintenance of trust relationships for sharing;
- Agile: supporting rapid change in business/mission requirements;
- Light-weight: can be reliably implemented with minimal additional administrative burden;



The key conclusions of this paper are as follows:

- There is no “one-size fits all” style of governance within federated environments. The style of governance must be tailored for the state or phase of evolution of a given federation as it forms and self-organizes.
- The end-game of the evolution of a federation formed for information sharing is information stewardship. Information stewardship is a best practice based upon empirical assessment of Information Technology (IT) governance and common practice within the public and private sectors.
- This paper defines the concept of a “meta-governor”. The role of a meta-governor is to guide federations through their evolutionary processes toward information stewardship.
- The paper provides guidance, in the form of checklists, for meta-governance, federations, and information stewards. These checklists are at a high level. However, they provide direction for follow-on work by the AFEI in establishing detailed implementation guidance within each of these areas.

While the DoD is only part of a broader, extended federation, the work the DoD has done provides a context for a broader dialog.



Principle Authors Foreword

This paper represents an effort by the AFEI ISWG to provide actionable recommendations to our sponsors that are both supported by empirical evidence and reflective of best practices. That said, best practices for information sharing, in many ways, are still being defined. Empirical evidence is still being gathered. Hence, the paper represents the best efforts of a dedicated group of people focused on delivering a useful product to a customer in reasonable amount of time. This paper is not intended to be the end of a discussion. Rather, we hope that this is a beginning of one.

Comments, corrections, reactions to this paper are welcome. We will issue updates to this paper as we learn and the best practices for information sharing governance come into clearer focus. We also invite new membership to the ISWG – a self-forming, self-organizing, and self-regulating federation focused on information sharing governance.

Bryan Aucoin, Alanthus Associates

Jarl Magnusson, Det Norske Veritas



1. Introduction

1.1. Purpose

The purpose of this document is to provide recommendations for establishment of Information Sharing Governance to the Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO). This paper was developed by Information Sharing Working Group (ISWG) of the Association For Enterprise Integration (AFEI), an affiliate to National Defense Industry Association (NDIA).

1.2. Scope

The recommendations within this report apply to the Department of Defense (DoD) and between DoD and its mission partners. Based upon the direction of the DoD sponsor and the working group participants, the scope was set to address federations, to include but not limited to:

- The US Federal Enterprise
- Coalitions led by the United States
- The Information Sharing Environment with regard to Terrorism Information
- State, Local and Tribal partners inside the United States
- The Aerospace/Defense Community to include the Transglobal Secure Collaboration Program

This group of federations is referred to as the “Extended Enterprise”¹ within this paper.

¹ Enterprise is defined in the American Heritage Dictionary as “An undertaking, especially one of some scope, complication, and risk.” AFEI uses the term “extended enterprise” to mean undertakings that bridge multiple organizational boundaries, thus adding to the complexity and difficulty of the situation. See : enterprise. Dictionary.com. *The American Heritage® Dictionary of the English Language, Fourth Edition*. Houghton Mifflin Company, 2004. <http://dictionary.reference.com/browse/enterprise> (accessed: January 15, 2008).



1.3. Structure of This Paper

The paper is organized as follow:

Section 1 Introduction	Provides the purpose and scope of the paper and describes its organization.
Section 2 - Statement of Need	Provides a concise description of the issues to be addressed by this paper.
Section 3 - A Vision for the Future	Provides a description of a “target state” for governance within the Extended Enterprise.
Section 4 – Transition – The Checklists	Provides checklists for governance authorities at the levels of the Extended Enterprise, communities of interest and practices (the self-forming federations), and for information stewards.
Section 5 – Recommendations for Follow Activity	Provides a list of recommendations for follow actions that are beyond the scope of the original tasking to the AFEI ISWG.
Appendix A - References	
Appendix B - Definitions	



2. Statement of Need (Current State)

2.1. *An Imperative to Continue Progress*

"We must recognize that we are woefully incapable of storing, moving, and accessing information - especially in times of crisis."

Executive Summary of Findings: Page 1, Congressional Reports:
H. Rpt. 109-377 – A Failure of Initiative: Final Report of the
Select Bipartisan Committee to Investigate the Preparation for
and Response to Hurricane Katrina

"For purposes of this Strategy, information sharing is defined as, 'Making information available to participants (people, processes, or systems).' Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant."

DoD Information Sharing Strategy

An enormous amount of information is shared across the Federal Government, State, Local and Tribal entities, with international partners and with the private sector and academia. All of these entities are dependent on timely, accurate and easily accessible information, and there are numerous examples of best practices, including:

- Environmental Protection Agency Water Data
- Department of Interior's Recreation One Stop
- Amber Alerts
- National Oceanographic and Atmospheric Administration Weather and Oceanographic information
- Child Exploitation Tracking System (in Canada)

That said, while these communities share information routinely, information sharing is not routine. There are still intrinsic barriers.

All organizations within the Extended Enterprise create information in the course of their normal operations. Yet, in many instances, information is not created, stored or managed in a way that enables its reuse outside of the organization, irrespective of the potential value of this reuse. Information and its reuse should be independent of the processes that create it or the original purpose for which it was created.



The issue before us is to determine how to overcome the policy, cultural, governance, resources and technological² obstacles, so that sharing of data and information is enabled, allowed, endorsed and encouraged throughout the extended enterprise.

Our *Service for Citizens*³ demands that we address these considerations. We must manage increased complexity, shorter lead-times, flexibility/agility, greater transparency, better security, greater situational awareness and accountability. This, in turn, drives an increasing need to share data and information. Examples include:

- Fighting terrorism (Information Sharing Environment, DoD, DHS, Intelligence Community)
- Climate change (Academia, Federal Government)
- eGov programs (Federal, State and Local Government)
- 24-hour authorities⁴ (Federal, State and Local Government) in Scandinavia

The sections that follow offer a series of perspectives on the current states of our governance, our culture, our policy, our management of resources and our technology and infrastructure. We will define a high-conceptual framework to allow us to understand and assess our current state. Whereas the focus of this report is on governance, we will focus on that consideration first.

2.2. Governance Needs

As stated in the DoD Information Sharing Strategy, we must address a number of considerations, to include:

- **Governance:** The means for coordination, regulation, orchestration and decision making within federations that are self-forming and self-regulating.

² These five dimensions: *policy, culture, governance, technology and resources*, are introduced in the DoD Information Sharing Strategy and form as basis for analysis within this paper.

³ **Services For Citizens** is the focus of the Federal Enterprise Architecture Business Reference Model (FEA BRM). The term encompasses the mission and purpose of the United States government in terms of the services it provides both to and on behalf of the American citizen. It includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of the Federal Government to the benefit and protection of the nation's general population.

⁴ The term "24-hour authorities" refers to integrated services (across the government) that are open to serve the public 24-7. These services are web-based and are built to share information and enable services to citizens (e.g. applying for a driver's license).



- **Policy:** The formal statements of intent and plans of action that DoD and affiliated organizations use to guide decisions and achieve rational outcomes. This includes legislation, regulations, and the requirements for processes, procedures and compliance.
- **Culture:** The patterns of human activity; the modes of acceptable behavior within an organization.
- **Economics and Resources:** The management of costs and benefits associated within information sharing evaluated in relationship to DoD Mission/Business priorities.
- **Technology and Infrastructure:** The information sharing capabilities, in the form of networks, databases, applications and other automated tools that enabling storage, access, sharing/exchange and discovery of information.

2.2.1. Governance and Culture

“Successful information sharing requires a major cultural shift across the DoD. There is an established mindset of information ‘ownership’. The new mindset must be one of information “stewardship”. The best technology, processes, and policies will not make this successful if the people do not embrace the new cultural norms.”

DoD Information Sharing Strategy

In many ways, culture arises from the application of a series of incentives over a period of time. Hence a review of how a culture has emerged is beneficial to defining a way ahead. In many medium-to-large enterprises, applications development is typically tightly bound to an organization that supports a particular line of business. Multiple application development shops support these different lines of business, even when applications development has been consolidated into a single organization. Also, typically, data (and information) is tightly bound to the applications that use them, even when separating data from applications is recognized as industry best practice.⁵

⁵ See *The Three Pillars, an Adaptation of Information Management and Data Quality*, by Bryan Aucoin, Panel 1, proceedings of the Eighth International Conference on Information Quality, (ICIQ-03) The concepts in Section 2.2.1 are substantively based on this paper. (http://colab.cim3.net/cgi-bin/wiki.pl?DataReferenceModel_09_2004/TheFootnotes_DRM_Vollv1#nid2IU)

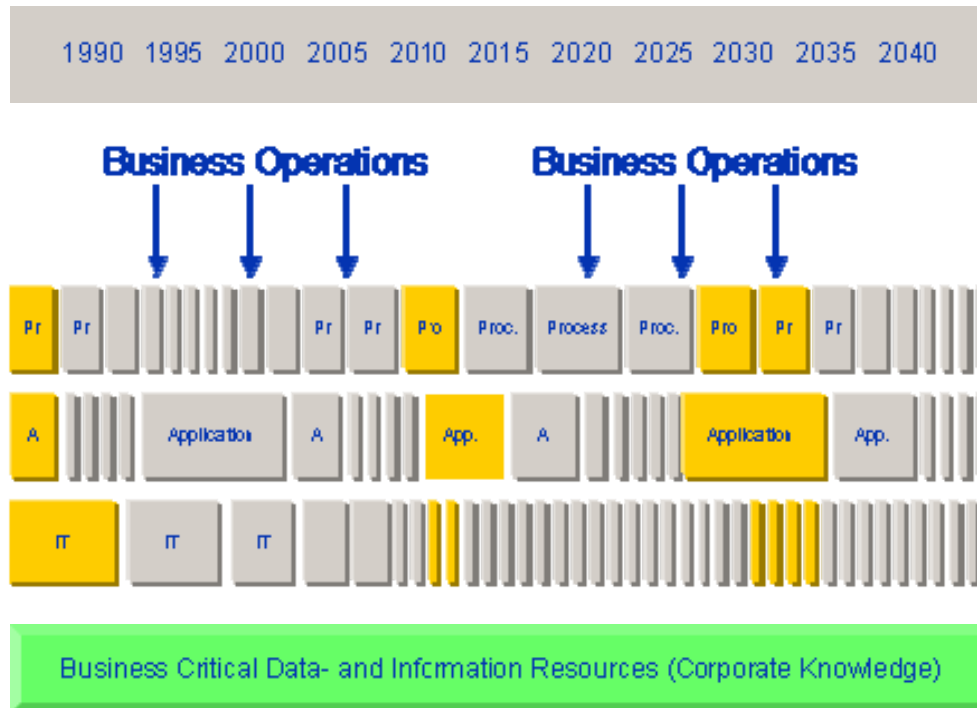


Figure 2.1 – Evolution of Information Management

Processes, applications and information technology change regularly, but information resources are more stable and intact over its lifecycle, here 50 years. We know that users need to access information through currently available processes, applications and technologies (yellow marked areas). Information needs to be de-coupled from these dependencies, in order to be shared, flexible and agile over time.

However, if we look inside each organization and its corresponding information technology (IT) support organization(s), we will typically find heavy investments in "vertical" information technology. The line organizations will have one or more large "ERP⁶-ish" systems that support the core business processes. Over time, new business requirements drive new information requirements. Many times, "local" IT support staffs are driven to respond quickly to their customers' requirements. Because updating large applications requires more time and resources, the IT organization will create additional small applications (and databases) in order to be responsive. Usually, data must be interchanged between the large application(s) and the small applications, or data is simply re-keyed into the smaller applications, resulting in a web of interfaces and redundant work.

⁶ i.e. Enterprise Resource Planning

Usually, requirements for information access and interchange emerge as the enterprise attempts to better manage available resources, improve processes, make informed decisions and chart direction. Again, the IT organizations create a web of interfaces to transfer and translate data to support executive information systems, integrated business processes and so on. A variety of approaches are used: data warehouses/data buses, batch processes, and middleware.

The evolution above tends to result in a number of outcomes:

- **Data are not generally created to support enterprise needs.** There are typically technical and political boundaries that inhibit this. To "line" applications development organizations, enterprise-level requirements for data are typically viewed as "external", as their direct customers, and typically the sponsor of the application, is not rewarded for serving the greater good, but for locally optimizing the performance of their organization.
- **Even when data are shared, they may not be fit for reuse within the Enterprise.** Assuming the political and technical issues surrounding the sharing of data can be resolved, the differences in the data themselves constrain their usefulness. Data produced to support a particular organization may not meet the enterprise-level requirements for currency and consistency. Further, definitions differ and it may be that no amount of calculation will resolve the semantics.
- **Data Quality becomes the issue:** This brings us to data and information quality. All of the dimensions of data quality may be satisfactory from the standpoint of people responsible for creating it. In fact, one can make an argument that for any given system, a core set of data maintained within that system must be of sufficient quality, otherwise, the system could not be used. However, when the data are made available for broader use, the quality of the data as perceived by the information consumer is much less.

From an information technology standpoint, the evolution described above leads IT service providers into an "O&M⁷ box canyon". The service providers must maintain their core systems, they must maintain the tactically-focused small applications deployed to support an urgent customer need. (And, the customer has come to rely on these applications as parts of daily business.) Changes to applications affecting shared data require modification of the web of interfaces, and are very expensive. The service provider has no funding to transition the small applications to a more robust platform. The customer will not fund a major new IT effort, is

⁷ i.e. Operations and Maintenance



demanding more fast tactical solutions, and is wondering why it takes so long to make seemingly minor changes.

In summary, the current culture for information sharing can be characterized as follows:

- A parochial perspective of information creation and use. In general, information is created and maintained with little regard to the potential for “external” inter- and intra-enterprise reuse.
- A reactive approach to information sharing. Capacity for information sharing is not built in “from the ground up”, but is addressed based on immediate business requirements in the most expedient manner.

Culture is about incentives. Hence, the major need we must fulfill is the establishment of appropriate incentives, through governance to treat information as a shared resource.

2.2.2. Governance and Policy:

Two factors are propelling the interest in information governance. First, a raft of recent federal regulations has made it a top priority for companies to better account for how information is being handled within their organizations. Laws such the HIPAA, FSMA and SOX⁸ mandates audits and controls. Numerous post-Sept. 11 security demands are required from the government. Businesses facing litigation are frequently subpoenaed for information. With all these directives involving their data systems, executives who fail to govern the information their companies maintain, or access, can no longer use ignorance as an excuse.

The second factor is more daunting because it involves much more than just learning to follow regulations. After three decades of aggressive computerization, companies are drowning in data and information. People produced about five exabytes of new information in 2002, twice the amount created just two years earlier. About 92 percent of this new information is stored in magnetic media, primarily hard disks. E-mail contributes at least 500 times more data each year than the amount generated by new Web pages.

Information governance programs are an attempt to corral all of this information into a useable form, an ambition that so far has eluded most organizations. This is no easy task. Our ability to store and communicate information has far outpaced our ability to search, retrieve and present it. Information management may turn out to be one of the major challenges of the new century.

Trend: The New Rules of Information Management, by Jeffrey Rothfeder⁹

⁸ Health Insurance Portability and Accountability Act (HIPAA), Financial Services Modernization Act (FSMA also known as Gramm-Leach-Bliley) and Sarbanes-Oxley Act (SOX).

⁹ Article in CIO|Insight, May 15, 2006, Jeffery Rothfelder, <http://www.cioinsight.com/article2/0,1397,1962565,00.asp>



For the purposes of this white paper, the term “policy” includes legislation, regulations, and the requirements for processes, procedures and compliance within the Extended Enterprise. Today, enterprises define and implement policies for information sharing with varying degrees of success. In general, enterprises do not have systemic means to:

- Identify extant policy related to a particular domain of endeavor.
- Reconcile those policies across the respective authorities for those policies.
- Manage sensitive information. Enterprises restrict access to information for good reasons and bad. They include privacy, protection of sources and methods, protection of proprietary information, and protection of program budgets and autonomy.
- Account for information assets, their value, cost and the cash-flow (or benefits) they provide to the enterprise.

Hence, the need that we must fulfill is a coherent strategy for management of information policy within the extended enterprise.

2.2.3. Governance and Resources

“The only ‘shared’ resource in the Federal Government that I see is money, and the apparatus to do that is enormous.”

- Jarl Magnusson

There is a human predilection to guard what is “ours”. The information we hold and the resources we use to create it are no exception. Further, we use a classic industrial-age mindset toward the implementation and management of information systems and the information that they create. As discussed above, individual agencies/organizations are not motivated to treat information as a shared asset.

While not wittingly, the Federal Budget Process reinforces a “stovepiped” approach to information sharing and access. Consider that the Federal Budget is organized around budget lines. The primary expectation from Congress and the Office of Management and Budget is that the agency assigned the funds will execute the budget in accordance with the intent of the line. The agencies implement the lines as programs. Programs, by their nature, tend to be parochial in their allocation of funds, particularly as regards to information sharing.

There are a number of disincentives for any given program to devote resources to information sharing:



1. First, to a program manager, information sharing looks like “charity work”. Sharing information beyond the scope of the program costs money, but is not directly accretive to the mission of the program. There is a prevalent fear at all organization levels of “unfunded mandates”.
2. Information shared poses a risk in the sense that it creates the prospect of uninvited critique, review, evidence for litigation, and so on.
3. To a program manager, requirements for common standards are “external requirements”. While compliance with a standard may save time and resources, the facts are that such compliance will cost time and money in education. Standards may also be more complex to implement for the particular task at hand. Further, there is the question of the testing and certification of compliance. This is not to say that program managers will avoid standards at all cost. Rather, they will assess the benefit verses the risk. Remember, a program manager is incentivized to deliver on time and on budget per customer requirements. His/her tenure may be two to five years. The fact that the system they manage may last 20 years and *may be* difficult to integrate in the last 15 of those years is not a compelling argument for a program manager to change his/her behavior.

Hence, organizations assume risks with little to guarantee added value to their mission or business. Attempts at allocation of resources within organizations have failed for the most part because of these disincentives. OMB and Congress are attempting to identify areas of redundancy, then integration and consolidate (e.g., e-Gov). However, this is a long term, incremental effort.

Management of resources is the critical area for decision. So the need becomes: “How do we reframe the debate about allocation of resources to support information sharing in the context of supporting shared mission/business requirements.”

2.2.4. Governance and Technology

“The federal government is the largest purchaser of information technology in the world by far. One would think we could share information by now. But Katrina again proved we cannot.”

Executive Summary of Findings: Page 1, Congressional Reports:
H. Rpt. 109-377 – A Failure of Initiative: Final Report of the
Select Bipartisan Committee to Investigate the Preparation for
and Response to Hurricane Katrina

Despite the plethora of technology products and services on the market today that purportedly solve the “information sharing problem”, the problem, seemingly though sheer obstinacy, persists.



People, Process and Technology

In the authors' opinion, while technology is an enabler, there are (too) many right answers to enable information sharing.

Hence the need is for a concise implementation sharing architecture. The point of such an architecture is to limit implementation options so as to optimize interoperability and flexibility for the enterprise as a whole.



3. Vision for the Future

“Deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment. “

- DoD Information Sharing Strategy

The DoD Information Sharing Strategy establishes a number of goals that describe the interrelated concepts needed to move the DoD from the current state of information sharing to the vision. The information sharing goals form an environment across the DoD that will:

- Promote, encourage, and provides incentives for sharing.
- Achieve an extended enterprise.
- Strengthen agility
- Ensure trust across organizations.

The DoD Information Sharing Strategy offers the following approaches to achieve these goals:

- Recognize and leverage the Information Sharing Value Chain.
- Forge information mobility.
- Make information a force multiplier through sharing.
- Promote federated information mobility
- Address the economic reality of information sharing.

The purpose of the sections below is to describe a target state that will offer a means to implement these goal and approaches.

3.1. A Framework for Governance

There are a number of key aspects of governance that must be addressed to successfully implement it within large, federated environments. These aspects relate more to how federations form, self-organize, and how they evolve once they form. Any group of federations will go through successive stages in governance approach. Our premise is that governance must be tailored to fit the extant evolutionary stage of a federation (or enterprise), or that governance will fail.



The first subsection below provides an overall framework for how such governance evolves as organizations mature. The purpose of this subsection is to describe the various levels of evolution and delineate the appropriate styles of governance to be used in each.

We introduce the term “meta-governance” to mean the governance of governance. Given that different styles of governance are appropriate depending on the stage of evolution of an organization, then a “meta-governor” can be used to guide self-forming federations through their evolution. Alternatively, a group of federations may form a meta-governance approach to guide the member organizations toward improved interoperability and information sharing. *We believe this describes the role of ASD (NII)/DoD CIO in the orchestration, coordination and management of federations within the Extended Enterprise.*

With meta-governance, we can guide the evolution of the federations toward best practices. The next subsection describes a synopsis of the work of Dr. Peter Weill and Dr. Jeanne Ross in *IT Governance, How IT Performers Manage IT Decisions for Superior Results*, (Reference [1]). In this book Weill and Ross did an empirical analysis of best practices in IT Governance based on measured outcomes in 256 enterprises. The specific outcomes measured were in Growth in Revenue, Asset Utilization, and Profitability. It is not the authors’ contention that IT is equivalent to Information Sharing. However, it is the authors’ contention that Dr. Weill’s and Ms. Ross’s work provides a series of “guide posts” for what must be governed and appropriate best practices for the styles of governance to be used in the a “target state” – the target in the evolution of our federations.

3.1.1. The Evolution of Concepts and Their Governance

Our premise is that any concept, whether is related to information technology, information sharing or any other realm of knowledge, transitions through a series of evolutionary phases within a human population over time. In short, concepts have a life cycle. Fostering concepts through that life cycle requires different styles of governance at each phase of that cycle. With an understanding of these phases, a “meta-governor” can foster innovation, speed education and adoption, and assimilate new concepts into infrastructure as expeditiously as practicable.

Consider the creation of the Internet. People at DARPA recognized that tying computers together using a common, simple communications protocol was a good idea and started building networks. Through the 1970s and 1980s this concept took root. Others copied the basic concepts and extended it by creating a wide range of network protocols - TCP/IP, DecNet, IPX, Banyan Vines – all were instantiations of the basic Internet concept. We had the “protocol wars” of the

1980s, and communities formed around these various standard work to expand their influence and market share. When networks had to be connected, the communities who used these various protocols had to negotiate at their “boundaries”. By the late 1980s and 1990s, the economics of supporting multiple protocols drove a common consensus within the Internet community: TCP/IP and its related family of protocols became the de facto standards, and these standards are managed for that community by various international organizations. They have become the stewards.

This type of evolution, as well as appropriate styles of governance, is depicted in Figure 3.1 below.

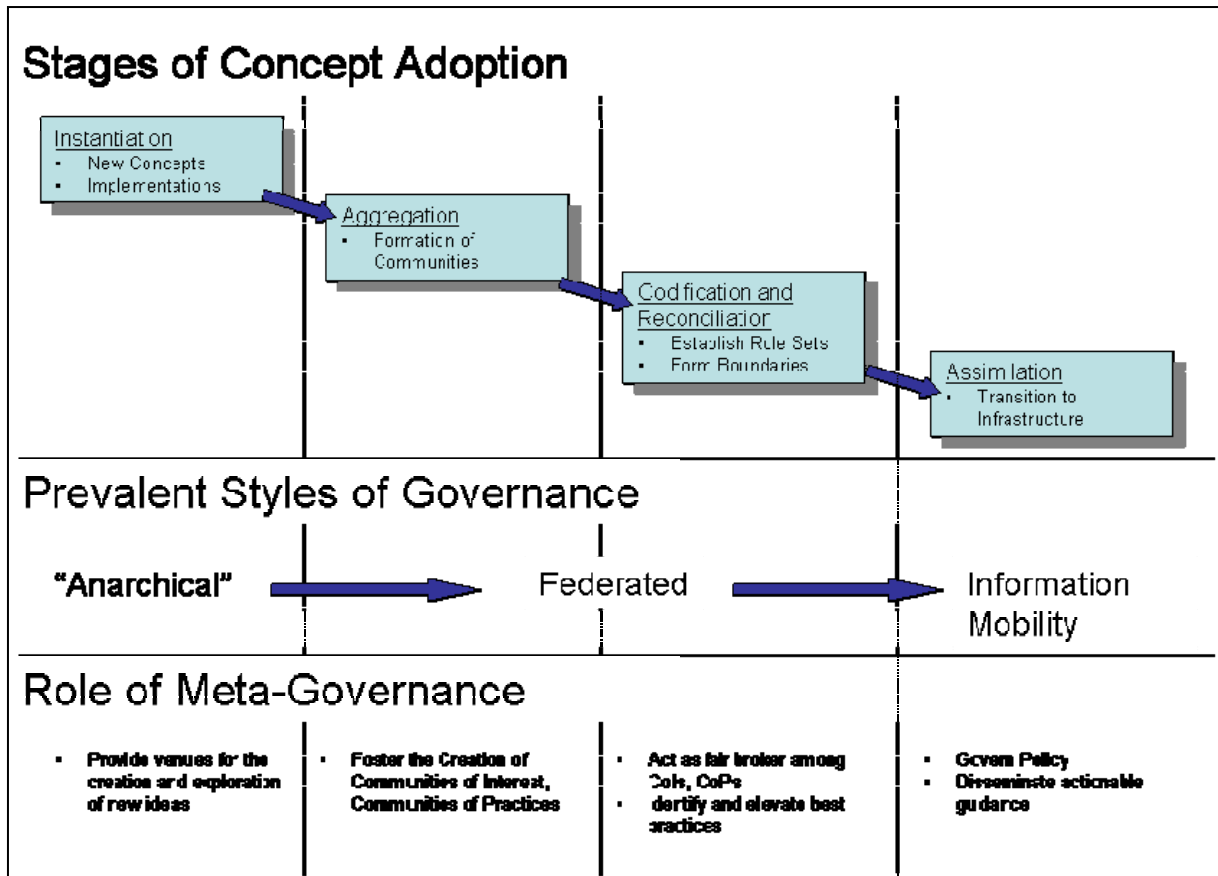


Figure 3.1 Concept Adoption and Governance

The basic stages of concept adoption are as follows:

- **Instantiation:** New concepts are created in the instantiation phase, generally from the synthesis of other concepts, but in new ways¹⁰. This is the creation of the new “model.” It occurs most often in places where people with different ideas congregate. In essence, the presence of many ideas provides a ready medium for synthesis. The second part of instantiation is implementation. This occurs when someone develops an instance of the model.
- **Aggregation:** The next phase is aggregation. This phase is characterized by: Adoption, Growth of Communities, and the Formation of Boundaries. Communities begin to form around the concept and they begin to establish common vernaculars, codes of conduct, decision making processes, and best practices. One concept may lead to multiple, different instantiations within different communities. When these communities interact, they must negotiate the differences between their respective instantiations.
- **Codification and Reconciliation:** In this stage, the concept has become embedded in the common consciousness. Most people have accepted that new rules have emerged, internalized them, and reconciled themselves to adopt an instantiation. Boundary conditions have formed, and the “wars” have started at the margins over which model within a number of models will be instantiated.
- **Assimilation:** Assimilation occurs when solutions become commodities and are taken for granted. We no longer think or argue about the concept. The concept becomes “infrastructure.” We define and build upon a unified rule set to govern that infrastructure. As an example, we no longer think about using plumbing, the telephone, or the Internet, we just use them.

The middle line of Figure 3.1 delineates the prevalent (and appropriate) style of governance at each particular level of organizational maturity. An anarchic style is characterized by decision making by individuals or small groups. A federated style is characterized by a combination of stakeholders agreeing by consensus. The informational mobility style is characterized by “centralized” making of binding decisions for a small but necessary set of principles, standards and practices.

The bottom line of Figure 3.1 delineates the primary role or function of a meta-governor during the evolution of a concept and communities that form around them. To foster innovation and

¹⁰ The *Medici Effect, Breakthrough Insights at the Intersection of Ideas, Concepts & Cultures* by Frans Johansson provides an excellent discussion of environments that foster new concepts.

instantiation, the meta-governor should provide venue to exchange information and ideas. Once ideas have transitioned into implementation, and those instantiations are being applied to support business/mission functions, the meta-governor should foster the creation of Communities of Interest (Cols) and Communities of Practices (CoPs), the self forming federations described within the DoD Information Sharing Strategy. Over time, and when necessary to support improved business/mission performance and utilization of resources, the meta-governor should act as the “fair broker” between Cols and CoPs and guide them toward common solutions and binding decision making (i.e., stewardship).

3.1.2. Best Practices for Information Technology Governance

Now that we have addressed in a generic sense how to manage the evolution of new concepts and self forming federations, we must now address the target state of what should be governed, and how to guide the evolution toward that target state. As a point of departure, the authors analyzed best practices for IT Governance, understanding that what we learned must be extensible to Information Sharing.

Reference [1] provides answers two core questions related to IT Governance.

- What should be governed?
- What are the best governance styles to apply to achieve desired outcomes?

Regarding the first question, based on the empirical analysis, Reference [1] poses the following key domains for decision making:

- IT Principles: Clarifying the business role of IT.
- IT Architecture: Defining the integration and standardization requirements.
- IT Infrastructure: Determining and enabling services.
- Business Application Needs: Specifying the business needs for purchased or internally developed applications.

The styles of governance delineated in Ref[1] include:

- Business (/Mission) Monarchy: Decisions are made by top business (/mission managers)
- IT Monarchy: IT specialists make the decisions.
- Feudal: Each business unit makes independent decisions
- Federal: Combination of the corporate center and the business units with or without IT people involved
- IT Duopoly: IT group and one other group (e.g., top management or business unit leaders) make decisions.
- Anarchy: Isolated individual or small group decision making.

The “Business Monarch”, “IT Monarchy” and “IT Duopoly” are styles of stewardship as described in this paper.

- IT Investment and Prioritization: Choosing which initiatives to fund and how much to spend.

Reference: [1] is a comprehensive work. We will not attempt to address each of its aspects at length. Application of the Reference [1] findings will depend on the specific organization or federation. However, the key conclusions from our analysis of Reference [1] and the evolution of concepts discussion above are:

- Information is a shared asset and should be managed as such. While information is not equivalent the information technology used to create, store and process it, there are distinct parallels and interdependencies between the two. Specifically, both are assets that should be managed at an enterprise-level and built for reuse.
- As a **target state**, the meta-governor should guide federations toward strong governance – towards stewardship.
- The specific things that need to be governed in the target state for information sharing parallel information technology.
 - Information Sharing Principles
 - Information Sharing Architecture
 - Information Sharing Strategies
 - Information Sharing Needs
 - Information Sharing Investments

However, the best practice patterns of governance in each of these domains has not been codified into a coherent set of reusable practices. Whenever we create a new enterprise, a community of practice or interest, we recreate a pattern, most times from whole cloth. We have difficulty reconciling different styles of governance within larger, federated enterprises, and there are no standard sets of guidelines established for implementing governance.

These conclusions are reinforced by the effort to create the Federal Enterprise Architecture (FEA) Data Reference Model version 2.0 (DRM 2.0). The DRM, in part, is premised on the concept that a three pillar strategy is required for any successful data/information sharing effort. The three pillars are:

- *Governance: Driven by Business/Mission Requirements.*
- *Data Architecture: The semantic and syntactic standards for the data to be shared.*
- *Information Sharing Architecture: A set of architectural patterns that allow information interchange and access.*

Within the DRM 2.0 Management Strategy conventions, the Governance Pillar includes the definition of principles, and the investments for information sharing. The Data Architecture and Information Sharing Architecture Pillars include the information sharing architecture defined by our analysis. The information sharing strategy within the DRM context is to use the three pillars to effect information sharing.

3.2. Information Sharing Principles

“The right information, reaching the right user, at the right time, to the right purpose, with the highest possible quality, security and abiding to current laws, rules and regulations.”

The right information means that it is the information that is required to support decisions in a process, that its meaning is unambiguous, and that it is complete

For the right user means that those who need access have it, and equally, those who should not have access do not.

At the right time means that the information is available when decisions relying on it need to be taken.

For the right purpose means that the process for creating and maintaining the information is defined and followed so that the information is accurate, and consistent.

Information Resource Management Vision for Swedish Defense

Information is a national asset.

From the Federal Enterprise Architecture Principles

As stated in the DoD Information Sharing Strategy, the vision for information sharing describes “...a future state where transparent, open, agile, timely, relevant, and trusted information sharing occurs to promote freedom of maneuverability across the information environment. Successful accomplishment of this vision will result in efficiencies in operations, enhanced and shared situational awareness, and – ultimately – mission success.”

As stated above, Information Sharing Principles are some of the specific things that need to be governed within an information sharing federation. The following guiding principles were derived from the various source documents and are provided here as context and as a point of departure for federations in the definition of their specific principles.

3.2.1. Information is a valuable asset

Information can be regarded as an asset when it is used by an organization and adds value. The information should be available and adaptable to changing user needs regardless of why, how, where and when it was originally created and independent of what, how, where and when it was intended to be used.

Information assets contribute and add to an organizations value, due to careful management, storage, improvement, updates, changes, sharing and reuse over time. Information becomes an



economical valuable asset because of the collected economical value it contributes with over time is higher than the costs for creation and life cycle management. Information assets are different from other assets since information-assets don't lose value or disappear when they are used.

In theory, an information asset can be used by any number of times, by any number of users, without losing in value. On the other hand, information assets can lose their values extremely fast. If information has no meaning or use, or if it's not actual, updated, accurate, or if it's not delivered in time, or if we can't trust the information anymore - then it has little value.

Information Assets are strategic when they fulfill strategic needs. Certain information is of strategic importance for an organization. A commercial company should have access to all information on their products and customers; government organizations must have information on legislation, economy, intelligence, geography, etc. An organization's strategic information can be analyzed by looking at information exchange or flows between the functions within the organization and external parties. Information assets can be measured, controlled and managed by using and creating adapted metrics from information dimensions such as:

- Source related dimensions; objectivity, factual, accuracy and consistency
- User dimensions; timeliness, completeness, value added, semantics, accessibility and understandability
- Maintainer dimensions; syntax, structure, representation, portability, uniqueness, security

Information assets must be properly identified as important enterprise resources, and included in the accounting procedures, such as financial and annual reports. Managing and annually report on corporate information assets are today required for government and industry enterprises by various legislation and trade regulation, such as:

- Publicly traded companies must adhere to the Generally Accepted Accounting Principles (GAAP), and the Sarbanes-Oxley Act (SOX) related regulations and commensurate controls. Companies are committed to integrity in the reporting to shareholders and the prevention of insider trading. Corporations are committed to protect the privacy of personnel related information and they strive for individual accountability with information assets.
- Government organizations must abide to national legislation and regulation. For US federal (state and local) agencies must all abide to the Clinger-Cohen Act, to introduce an IT and Information Governance. The Federal Information Security Management Act, or FISMA requires federal agency compliance with information security best practices by



mandating that federal security executives must follow stringent accountability measures. Under FISMA, the Office of Management & Budget is charged with setting policies, standards and guidelines for every agency's information security.

3.2.2. Other principles and precepts

- **Standards Principle** - Information should have standardized structures and representations. Standard content (name, classes and definitions), context (business rules) and various types of associations will simplify interoperability, usage, quality and safety.
- **Information should be created once and used many times** throughout the life cycle. - In the shared data environment, sharing or reuse of existing data is the norm. Source Data is prepared or acquired one time. Data models and associated business rules ensure consistency of structure and content and a common understanding of the data. Commercial and international standards shall be applied.
- **All users should be positively identified.** – Building trust and accountability requires users to be identified. Anonymous access and usage should not be allowed. Data and information needs to be proven authentic. Access to information and the aggregation of information is governed by the strict adherence to protocols, which provide assurance and mitigate the potential for contamination and compromise of information.
- **Do what you do best** – Few government organizations are proficient in managing financial resources, therefore we are using neutral and independent banks. Networks and information systems can be outsourced to infrastructure capability providers. Data and information can like financial resources, be managed by external, neutral and independent “information banks”.

3.3. Target State Governance

“A comprehensive, widely understood governance framework is critical for creating and sustaining a federated information sharing community of organizations and individuals aligned to the information sharing vision and agreed upon rule sets and processes. The governance framework must articulate the accountability and authority; promote standards and guidelines; ensure a consistent well-defined approach, processes and procedures; adjudicate disconnects; establish legal and policy enforcement; and use performance measures to ensure progress towards achieving the information sharing goals.”

- DoD Information Strategy

Based upon the vision, the principles, and the analysis above, we believe that the governance construct for information sharing depicted in Figure 3.2 should be established within the Extended Enterprise:

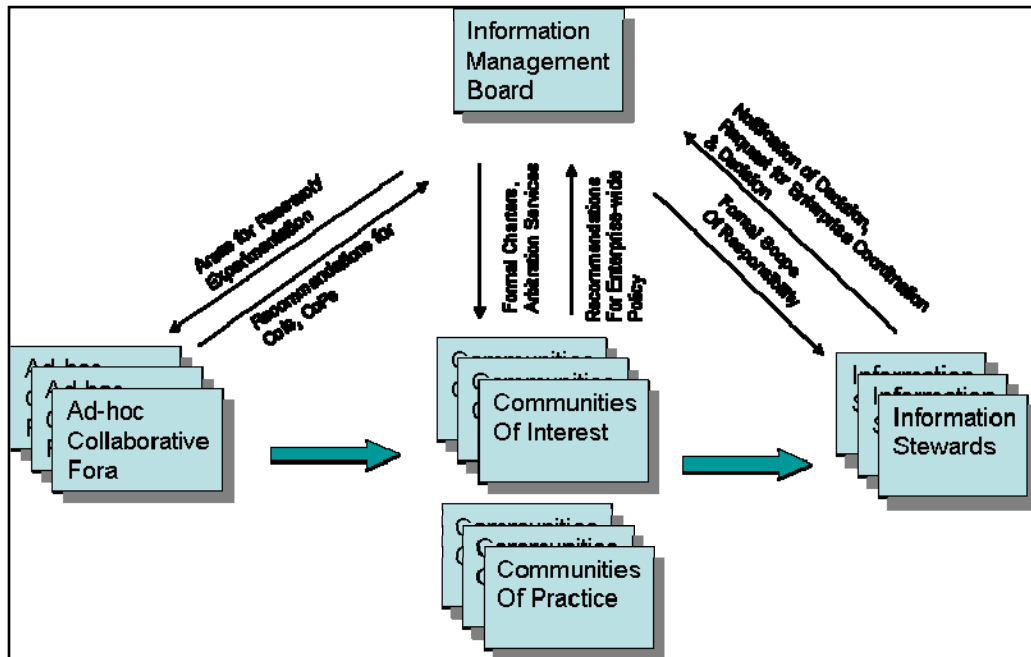


Figure 3.2 – “Meta-Governance” in the Extended Enterprise

Within this target state, the Information Management Board acts as the mechanism for “meta-governance” described in Section 3 above. It is responsible for *guiding* (not dictating nor mandating) the evolution of self-forming federations into formalized governance by stewardship over time.

This board provides the venues for the creation of collaborative fora to foster new ideas and innovations. Once communities form around new concepts and implementations, the board charters new Communities of Interest and Communities of Practice. These CoIs and CoPs can then begin to codify and reconcile implementation approaches. During this time the Board can act as the fair broker to mediate and arbitrate differences between communities. Finally, when a community has reached the necessary level of maturity, the Board would delegate authority for specific information to a steward, who would be responsible for leading that community. The Information Management Board would implement processes to:

- Promote standards and guidelines,
- Ensure a consistent well-defined approach,
- Adjudicate disconnects,
- Establish legal and policy enforcement, and
- Measure performance.
- Align current information sharing initiatives and programs.

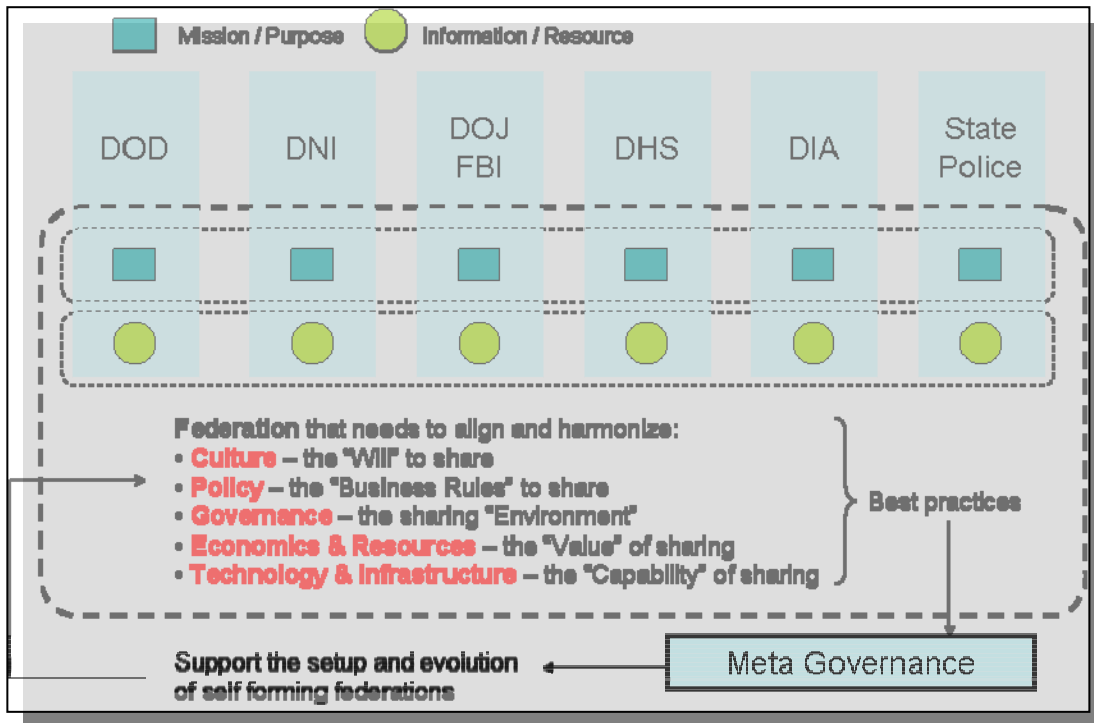


Figure 3.3 – Operation of Meta-Governance in a Large Extended Enterprise

The governance model above can be implemented at different organizational tiers within the extended enterprise:



- At the Federal level, in conjunction with the Federal CIO Council
- At the Department level (e.g., DoD)
- At the Agency level
- At the Program level (e.g., Joint Strike Fighter)

3.3.1. Using Governance to Effect Culture

“Successful information sharing necessitates a mindset where information is continually shared as a normal course of work. It begins when organizational leaders set the example and demonstrate their commitment by advocating for information sharing, and will be realized when the dissemination of information is supported at all organizational levels.”

DoD Information Sharing Strategy

As stated earlier, culture arises from the application of a series of incentives and indoctrination over a period of time.

The DoD Information Sharing Strategy provides the following guidance regarding the steps required to create a new culture:

- Influence all training curriculums from basic training to senior service schools.
- Train on tactics, techniques, and procedures (TTPs) that clearly outline information sharing approach and implementation plans.
- Require each information-sharing program or initiative to address the cultural considerations in implementation planning.
- Establish a trusted risk management environment (and mindset).
- Foster an environment to share information. Recognize leaders who promote an information sharing environment. Offer incentives to embrace information sharing and stewardship. Encourage participation in Communities of Interest.

Changing culture is the art and practice of indoctrination and defining incentives. In Table 3.1 below, we propose the aspects of a new information sharing culture as well as the training and incentives required to create that culture.



Transition From:	To:	Incentives	Governance Requirements
Organizations and staff are not aware of data- and information as critical enterprise resources	Organizations and staff are aware and trained to regard data- and information as critical enterprise resources	Build awareness Better decisions Improved DQ/IQ Improved security Personal career development	Provide basic education and continuous training for governance of data- and information resources Provide specialist training Provide executive training
Organizations hold information as private and proprietary. Information sharing is by directive.	Organizations make information available so users can search, retrieve and use trusted, shared information assets. Information sharing is by default.	Situation awareness Business Intelligence Corporate Knowledge Interoperability Harmonization Integration Reduce lead-times Reduce costs	Provide Information Sharing Policies Provide regulations and procedures on Information Sharing Make information available in a neutral, independent and trusted environment ¹¹
Organizations do not regard data and information as assets	Organizations govern data- and information as assets	Better visibility of info Traceability of info Improved DQ/IQ Cost control/awareness Build new capabilities for the organization Information Superiority	Provide metrics Provide accounting Provide in-valuation Provide quality criteria/s Provide control measure/s
Organizations exchange information through protected transmission of identified computers	Organizations share trusted information among trusted users	Building trust and safety Proven authenticity Trusted sharing Abolish anonymous users	Provide PKI Classify users Classify information Match users and information
Programs are “punished” if they share information with others	Programs will be “rewarded” if they makes their information available for others	Save time and money to search, retrieve info Reuse/save resources Be smarter Build new resources Build new capabilities	Automated procedures for procurement Simulated environments to support programs, SBA, SBD
Risk programs are fragmented and stove piped	Organizations can analyze holistic/enterprise risks, based on integrated and shared information resources	Building Risk Awareness Building Trust Building Agility	Provide risk “indoctrination” Managing Risk by Managing Information

Table 3.1– Creating a New Information Sharing Culture Policy (Cont)

¹¹ This is especially important due to cultural and other differences between organizations. The neutral third party function could be regarded as an “Information Bank”



Transition From:	To:	Incentives	Governance Requirements
DoD's sensitive information is protected by statute, and is very difficult to exchange/share with others	Shared Incentives for Information	Building access control Building security Building awareness Building traceability	Provide PKI Classify Information Classify users Match information and users
Technology empowers people	Information empowers people	Shift peoples views and perception on what's important in the organization	Gratify and promote people that make effective use of information
CIO is an IT manager	CIO is the chief "custodian" of information resources, and helps the organization to make the best possible use of data and information	Clear "Chain-Of-Command" Defined Carrier-Paths	CIO authority and responsibility CTO authority and responsibility Supporting executives and specialists
Communities are stove-piped and difficult to be connected. Approach is system integration.	Dynamic, self-forming "Communities of Interest" and "Communities of Practice", by focusing on information integration	Building Flexibility Building Agility Interoperability Short lead-times	Supporting rules and procedures for IPT's, sharing of resources
Numerous disincentives for Information Sharing. Information "owned" by people	Shared Incentives for Information. Information "owned" by enterprises	Less bureaucracy Possible automation of recurring processes Openness, accountability Fair competition Helping colleagues Reuse of previous efforts Enterprise responsibility Cost, quality, time control Invite oversight	New approach on administration, with automation, best practices, openness, new rules and regulations

Table 3.1– Creating a New Information Sharing Culture Policy (Cont)



3.3.2. Using Governance to Effect Policy

“Clear, concise and comprehensive guidance is necessary to implement this Information Sharing Strategy. Laws, policies, regulations, and business rules must be evaluated and adjusted, as required, to facilitate the flow of information across the federated information sharing community, including all external partners. Policies must be consistent and harmonized at multiple levels, including national and international laws and regulations that affect all federal departments and agencies; individual agency guidance for information sharing between and within agencies; policies guiding Federal, state, local and tribal relationships; and regulations affecting sharing and protection of information between government agencies and the private sector. Precise guidance will result in common methods and approaches, and promote both security and unity of effort.”

- DoD Information Sharing Strategy

Specific implementation activities will include, but are not limited to:

- Assess existing policy and guidance to address gaps and differences to improve information mobility.
- Reconcile diverse rules for information sharing among partners.
- Establish and promote a federated approach with all partners.
- Establish Trust – in people, technology, data, and processes.
- Develop and align policy. Establish consistent rules for sharing information. Establish simple and consistent rules for identifying, handling, and protecting controlled information.
- Promote sharing while preserving individual privacy protections and/or civil liberties.
- Influence planning and programming guidance.



Transition From:	To:	Incentives	Governance Requirements
Fragmented Information Sharing Policies	Coherent Information Sharing Policy that integrates laws, rules, regulations and practices within the government and with external partners	Clear requirements Clear intent, conops Build awareness and trust Unity of effort Improved quality	Evaluate, adjust and harmonize current laws, rules, regulations and policies Build common models, procedures and guides
Unclear ownership of information. Non-controlled IPR	Clear stewardship, IPR (including copyrights, protection of ideas, concepts, patterns, etc), Provenance and Authenticity	Clear stewardship The right to use Traceability Reimbursements, royalty Build trust Less litigation	Tag information PKI User Policies/Certificates User Identification Classify Info and User Relate User and Info
No metrics and no control of information	Simple metrics are established, like zero-errors, zero-waiting, zero-problems	Information Governance grows as a discipline Understandable	Establish Information Governance Metrics
"Frozen" islands of information	"Mobile" Shared Information Resources	Information can be used for other purposes than it was intended for	Recorded usage Rules for identification, handling and protection

Table 3.2 – Governance and Policy

3.3.3. Using Governance to Effect Economics and Resources

“The DoD shall tie information sharing to the Department’s fiscal dimension. The QDR specifically directs that the Department will ‘...reach investment decisions through collaboration among the joint warfighter, acquisition and resource communities...begin to break out its budget according to joint capability areas...manage the budget allocation process with accountability ... (and) establish ‘Capital Accounts’ for Major Acquisition Programs.’”

- DoD Information Sharing Strategy

Specific implementation activities will include, but are not limited to:

- Incorporate information sharing objectives into the requirements, acquisition, planning, and budgeting processes (e.g., JCIDS, PPBS, acquisition process).
- Establish guidance and priorities within the budgeting and resource allocation process.
- Leverage synergy of combined investments with external partners



Transition From:	To:	Incentives	Governance Requirements
Data and Information is not a recognized asset, and therefore not part of budget, acquisition and accounting processes	Incorporate information assets and sharing objectives into the requirements, acquisition, planning, and budgeting processes (e.g., JCIDS, PPBS, acquisition process).	Improved executive understanding Improved control Correct accounting	Rules and directives on how to value and account for data and information resources Establish guidance and priorities within the budgeting and resource allocation process.
Need to better understand shared costs and resources with industry and allies	Leverage synergy of combined investments with external partners	Better cost control Contracting and acquisition	Value data and information in relations with partners and allies
No current value on data and information resources	Valued data and information resources	Improved contracting Cost control	Cost value Cash Flow valuation Price valuation
People information (staff, patients, students, travelers, retirees, leaders, etc) is fragmented and without strict control	People information is managed uniformly, with protection of privacy and civil liberties ¹²	Less redundancies Less inconsistencies Building trust Building security Protection Integrity	PKI Integration and harmonization of personal information Unified rules and regulations
Product information (platforms, weapons, buildings and other systems) is fragmented between contractors and services	Product information is integrated and harmonized among all users	Less redundancies Less inconsistencies Better DQ/IQ Improved security Flexibility, agility Improved Config. Mgmt Life-cycle approach Traceability Less costs and lead-time	Product information to be managed by independent, neutral third party that implements required standards, models and architectures

Table 3.3 – Governance and Resources

¹² The Personal Data Act of Sweden states that personal data can only be registered and used if the actual person who is registered gives his/her consent, and if the usage is according to current legislation, or if it is necessary to close a contract with the registered person, or if it is needed to fulfill a legal obligation, or if it is to protect a major interest for the registered person, or if it is of national interest.



Transition From:	To:	Incentives	Governance Requirements
Difficult to have oversight of budgets, acquisition and planning, especially across programs and organizations	Integrate information among war fighter, acquisition and resource communities. Provide automated procedures to support investment decisions and oversight of programs	“Net-Centric” administration and bureaucracy Automation Best practices	Financial information to be harmonized among services and organizations Financial-, program- and product information to be reached as SPOE Develop best practice rules to information resources
Limited ability to change methods for accountability	Immediate transition of methods of accountability, on joint capability areas, resources, budgets, special, accounts, readiness, mission specifics, coalitions, investments, research, infrastructure, etc	Integrated and harmonized information can be cut and presented in numerous ways Adapted results depending on user	Administrative information to be integrated, harmonized and shared among organizations

Table 3.3 – Governance and Resources (Contd)

3.3.4. Using Governance to Effect Technology

“Enabling information sharing through the use and practice of current technology and the exploitation of potential future technology allows for improvements to the assured flow, management, and processing of information. The DoD will leverage the many investments it has made, and will continue to make, within the net-centric and the information technology (IT) environment. The DoD will work with external partners who have highly developed technology support for information sharing while maintaining capabilities to work with external partners who have limited or no technology support for information sharing.”

- DoD Information Sharing Strategy

An enormous amount of work has been done since 9/11 on technology to enable information sharing. We believe that we are now ready, as an Extended Enterprise, to begin to limit implementation options verses creating new ones. Using the concepts detailed in Section 3.2.1, we believe we are in the process of Reconciliation and Codification, moving toward Assimilation. The DoD Information Sharing Strategy lists a number of implementation activities/goals that must be addressed:

- Comply with the DoD Enterprise Architecture and Federal Enterprise Architecture guidance.



- Implement federally compliant strong identity and access control. Conform to the Federal Identity Management Federation standards. Advocate technically equivalent solutions with other external partners.
- Implement existing DoD and Federal technology strategies.
- Apply technology to improve information mobility by requiring trusted information to be visible, accessible, and understandable to any authorized user in DoD or to external partners except where limited by law or policy.
- Participate in developing, promoting, and enabling use of standards by partners.

We view that there are four components of the target state vision for information sharing architecture required to realize these goals within an extended and federated enterprise:

- Data Sharing Architecture: The services that we deploy to transfer and access data.
- Data Architecture: The semantic and syntactic descriptions of data.
- Identity Management: Identity management is critical for the management of access to information in accordance with an access management policy.
- Policy/Attribute-Based Access Management: The capability to define, codify and deploy access management policy into a Service Oriented Architecture.

If we view information sharing as a “hierarchy of needs”, analogous to Maslow’s hierarchy, it provides us a context for establishing our direction. Such a hierarchy of needs is provided in Ref [2], the IC-DoD Data Services Reference Architecture. It is depicted below in Figure 4.1 (modified somewhat to reflect the nomenclature of the DoD Information Sharing Strategy).

3.3.5. Data Architecture and Data Sharing Architecture:

Figure 4.1 below provides an overview of the roles of data architecture and data sharing architecture within a federated environment. We will describe each layer in turn:

- Data Capture and Retention: To effectively share information, a federation must agree upon a common data architecture (common semantics, common syntax) for the data that the federation needs to share. Each member of the federation may have any number of data repositories, all with their respective architectures tailored to support the specific business/mission functions that each supports. However, as a target state vision, the federation should agree upon a common set of data architecture standards that are used to guide the mapping of data between databases, and guide the design of new data repositories. As an example, ASD(NII) in collaboration with the DNI CIO has initiated an effort to define a Universal Core – a

set of universal, basic data standards that answer the core interrogatives: Who, What, When, Where, and How.

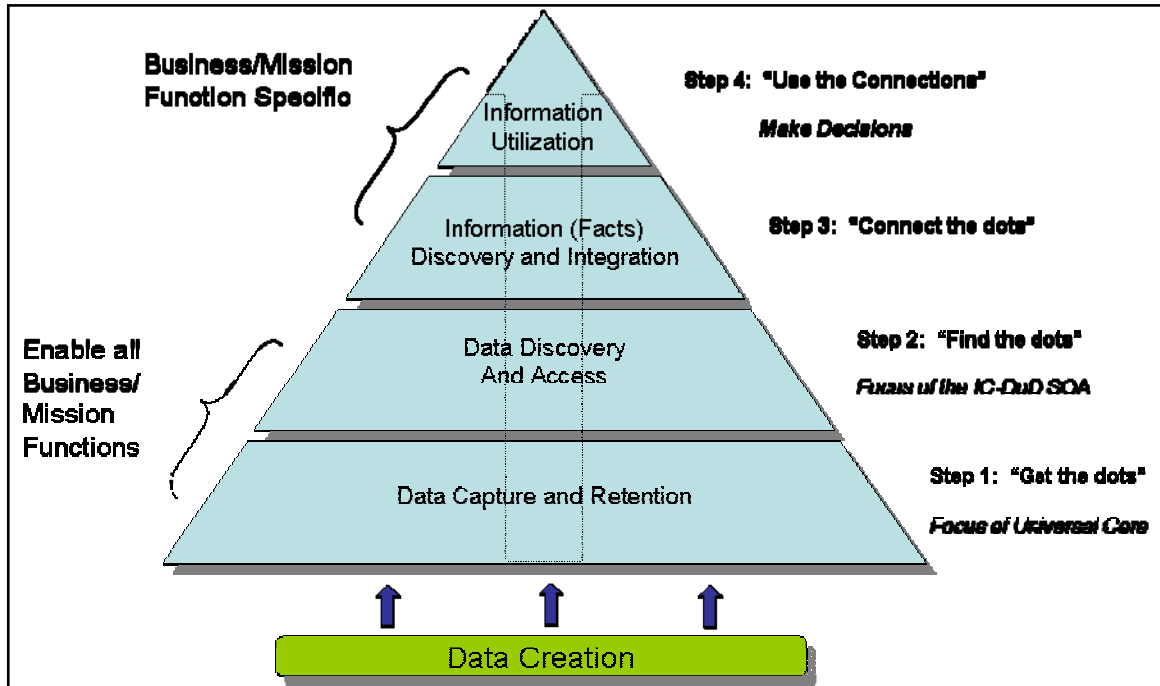


Figure 4.1 – Data Hierarchy of Needs

- Data Discovery and Access: Again, to effectively share information, a federation must agree upon common architectural approaches and patterns for searching federated information resources, retrieving information from them, subscribing to them and notifying information consumers when new information has been received or created.

Reference [3] provides a Data Supplier-to-Consumer Matrix that architects can use to determine which services should be provisioned to support a federation’s information sharing requirements. Alignment with Reference [3] ensures alignment to the Federal Enterprise Architecture.

Reference [2] IC-DoD Data Services Reference Architecture, and the associated service specifications are derived from the Reference [2] guidance and provide action guidance to developers for implementing these services.

- Information Discovery and Integration: Once a minimum set of information sharing infrastructure is in place (i.e., services for information discovery and access), the

federation can begin to provide the services for information discovery and integration (i.e., the derivation of new information from previously unrelated data.) These services may take any of a number of forms.

- Information Utilization: The value of information is measured in its use and impact. Once new information is discovered by the mission or missions, that information drive new actions and decisions.

Establishing appropriate standards and architectural patterns at the base of the pyramid enables flexible, scalable information sharing within a federation. A well defined, focused data architecture covering those things that are shared provides a means to capture data in a reusable way. A well defined data sharing architecture provides a common basis for data discovery and access.

3.3.6. Identity Management and Policy/Attribute –Based Access Management

Figure 4.2 depicts the relationship of identities and the policies used to manage access to shared data repositories.

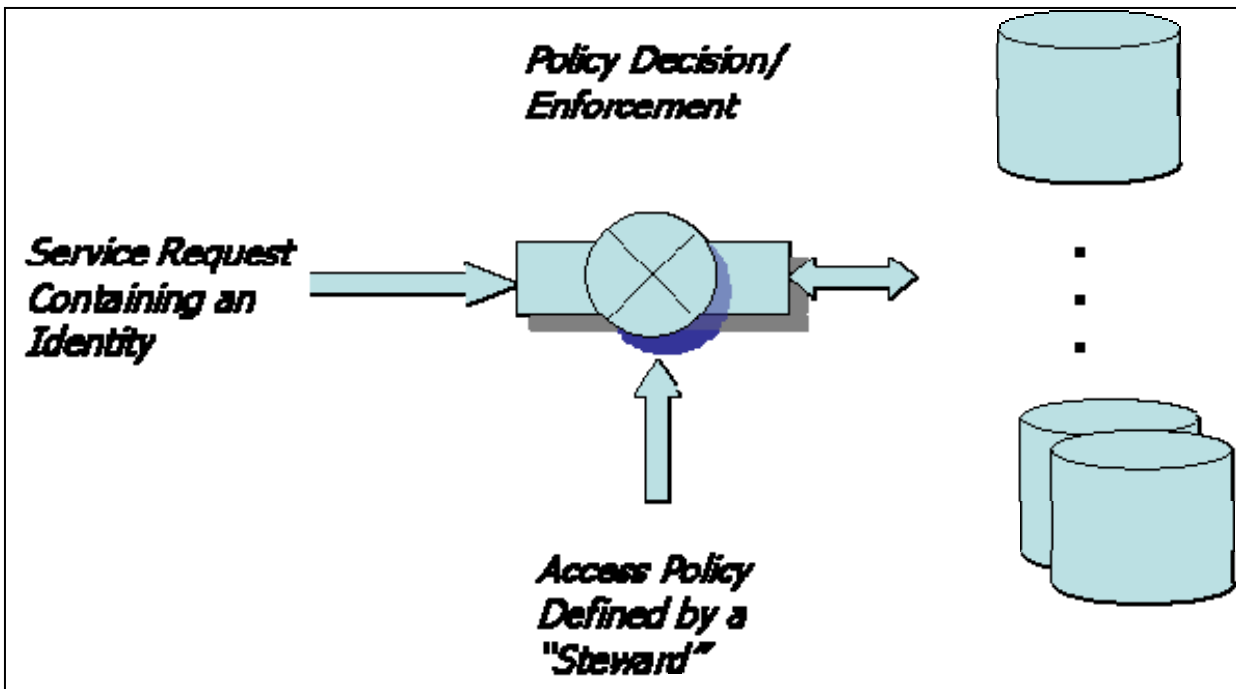


Figure 4.2 – Identities and Policy/Attribute-Based Access Management



Access to much of the important data within the extended enterprise must be managed. There are issues of privacy, protection of intelligence sources and methods, and the protection of proprietary information and intellectual property within the private sector.

As a general case, access to data is granted in accordance with a policy that may be expressed as a function:

$$\text{Access} = f(\text{user metadata, data object metadata, environmental metadata})^{13}$$

Access is dependent upon who the user is (i.e., his/her identity) and other related metadata, such as his/her position within an organization. It is also dependent upon the actual data themselves. Finally, access to data also may be contingent upon the network and/or physical location of the person requesting it. For example, in the Intelligence Community, a policy might dictate that access to data regarding the Iraqi insurgency may only be granted to Iraqi analysts logging in from their desktops in a secure location.

In short, policy/attribute-based access management of data within the extended enterprise will require: 1) a means of federated identity management; and 2) common constructs for access policy, including user metadata, data object metadata and environmental metadata.

It is the role of governance within the extended enterprise to establish these constructs.

Transition Technology From:	To:	Incentives	Governance Requirements
Disparate data architectures within the data repositories across the extended enterprise	A core set of common data standards and architecture for those data that are shared	Provides the basis for common understanding of the data	Data Architecture Governance
Disparate data sharing architecture within the extended enterprise	A common architectural pattern for data sharing within the extended enterprise	Provides the common basis for information sharing and discovery	Data Sharing Architecture Governance
Disparate definitions of "identity" and means of management	A common definition of "identity" and a federated means of managing them	Provides the common means of identification and authentication within the extended enterprise	Identity Management Policy
Disparate means of implementing access management	A common means of defining access management policy.	Provides the basis for federated access management	Access Management Policy

¹³ See the discussion of Attribute Based Access Control within *Special Publication 800-95, Guide to Secure Web Services, Recommendations of the National Institute of Standards and Technology*

4. Transition – The Checklist

The purpose of this white paper is to provide recommendations to the DoD sponsor for a “checklist” to implement information sharing governance within the extended enterprise. As described in the DoD Information Sharing Strategy, this governance must be tailored toward dynamic, self-forming, self-organizing federations focused on common mission/business needs.

This checklist will use the preceding chapters as its foundation, applying the concept of meta-governance to guide these self-forming federations through an evolutionary process toward best practices.

The section is divided into three subsections. The first section describes the activities and the things that need to be governed at the Extended Enterprise level. The next section describes the activities and the things that need to be governed at the Federation/Col/CoP level. The final section describes the things that need to be governed once stewardship is achieved. A justification is provided for each of the items of the checklist.

4.1. For The Extended Enterprise

Actions at the extended enterprise level:

4.1.1. Phase 0 – General:

This phase includes the actions required to establish meta-governance within the extended enterprise.

- Establish an Information Sharing Policy for the Extended Enterprise. At a minimum, this Information Sharing Policy should contain:

The roles and responsibilities of ASD(NII)/DoD CIO with regard to establishing meta-governance within the extended enterprise.

The roles and responsibilities of Communities of Interest/Communities of Practice (the self forming federations).



The roles and responsibilities of Information Stewards.

- Communicate Information Governance principles, structures and core procedures to senior management and to the organization at large.

These principles, structures and core principles must be governed within the Extended Enterprise per the analysis in Chapter 3. The indoctrination required to change culture within the extended enterprise.

- Train personnel who are responsible for the management of programs and the execution of funds in Information Sharing.

The indoctrination required to change culture within the extended enterprise.

4.1.2. Phase I – Instantiation:

- Establish venues for collaboration around information sharing needs.

Venues for collaboration support the Instantiation Phase described in Section 3.2.1. These venues permit stakeholders with common mission/business needs to identify one another and exchange new concepts and lessons learned regarding how to best meet those needs.

- Create a standing process for identifying and endorsing Communities of Interest and Communities of Practice (i.e., self-organizing federations) around mission/business needs for information sharing.

This process supports the Aggregation Phase. Once a community has formed around a particular mission need, such a process would enable: 1)Prospective members of the community to identify and join; 2)Empowerment of the community to perform prescribed functions under the auspicious of a sponsoring authority (i.e., ASD(NII)); and 3) Reconciling of roles and charters with other existing communities.

4.1.3. Phases II and III – Aggregation, Codification and Reconciliation

- Establish a process for creating a “fair broker” to reconcile and arbitrate differences between communities.

Federations will form around particular mission/business needs. The decisions and actions taken by any particular federation will be guided by and optimized for those particular mission/business needs. The decisions by one federation may therefore



negatively affect others, because the decisions do not encompass the equities of the entire extended enterprise. The “meta-governance” organization can act as a fair broker and ensure that the equities of the entire extended enterprise are addressed.

- Provide “boiler-plate” agreements to formalized governance within a Community/Federation.

These templates should be provided as an aide to new Communities of Interest and Practice to accelerate their formation. Such templates will provide “guide posts” to communities as they organize.

4.1.4. Phase IV - Assimilation

- Provide a process for selection, training and appointment of Information Stewards.

This process supports the Assimilation Phase. Once a Community of Interest or Practice reaches the required level of maturity, then the role of that Community can be formalized.

The things to govern at the level of the Extended Enterprise:

- Information Policy (including information governance policy)
- Information Sharing Principles

These principles provide a basis for decision making within the extended enterprise.

- Information Sharing Architecture

This information sharing architecture provides a minimal high-level set of guidance for members of the extended enterprise to ensure interoperable data exchange.

- Common Information Sharing Strategies

The extended enterprise should retain best practices as they are discovered to enable future reuse.

- Common Information Sharing Needs

The extended enterprise should orchestrate the focus of the federations to address common information sharing needs.



People, Process and Technology

- Common Information Sharing Investments

The extended enterprise should investments to address issues of common concern in a coherent way.

- Incentives for Information Sharing

The extended enterprise should define and implement incentives for information sharing.



4.2. For Federations, Communities of Interest, Communities of Practice

Table 4.1 below provides a synopsis of the actions that should be taken by self-forming federations (including communities of interest and practice) with respect to information sharing governance.

Item to Govern:	Action:	Purpose:		Incentives:	Extant Guidance:
		Transition From:	To:		
Need	Determine what needs to be shared. (Based on mission/business requirements) <ul style="list-style-type: none"> The way the Federation decides what the Federation Needs to Share 	Undocumented and under-documented needs	A coherent set of well documented information needs	Provides focus of allocation of federation resources around common needs.	<ul style="list-style-type: none"> Organization Objectives Federal Enterprise Architecture Data Reference Model (FEA DRM), Chapter 3
Charter (Self Regulation for Trust)	Establish Policy and Compliance Regime (e.g., a legally binding vehicle, MOAs, Contracts) <ul style="list-style-type: none"> Includes information sharing principles Includes Business rules 	<ul style="list-style-type: none"> No means to assess compliance with Federation Agreements 	Auditable means to verify compliance with Federation Agreements	<ul style="list-style-type: none"> Provides the basis of establishing and maintaining trust among for federation members 	<ul style="list-style-type: none"> National and International Laws Generally Accepted Business Practices ISO 9000 Series Certificate Policies and Practices Statements
Information Mobility Rules	Establish Information Access and Management Policy: The way the Federation decides what the Federation Needs to Share	<ul style="list-style-type: none"> Disparate means of implementing access management Static ACLs 	A common means of defining access management policy. Hybrid of ACLs and dynamic ABAC	Provides the basis for federated access management Controlled Info is only mobile to authorized users	<ul style="list-style-type: none"> Attribute-based Access Management (US DoD and DNI) HSPD12 (FIPS 201)
Information Preparation Standards and Rules	Establish Data Standards Agreements and Architecture Governance (gets the information ready to be shared) <ul style="list-style-type: none"> Marking/tagging requirements and definitions (handling instructions) 	Disparate data architectures within the data repositories within the extended enterprise	A core set of common data standards and architecture for those data that are shared	Prepares information to be mobile Provides the basis for common understanding of the data in order to share data accurately and unambiguously	<ul style="list-style-type: none"> Federal Enterprise Architecture Data Reference Model (FEA DRM), Chapter 3



Item to Govern:	Action:	Purpose:		Incentives:	Extant Guidance:
		Transition From:	To:		
Information Mobility Services	Agree upon the services required to make information sharable. (e.g., discovery, directory, collaboration)	Disparate data sharing architecture within the extended enterprise	A common architectural pattern for data sharing within the extended enterprise	Provides the common basis for information sharing and discovery	<ul style="list-style-type: none"> • FEA DRM, Chapter 5 • IC-DoD Service Oriented Architecture
Identities	Establish Identity Management Capability	Disparate definitions of "identity" and means of management	A common definition of "identity" and a federated means of managing them	<ul style="list-style-type: none"> • Provides the common means of identification and authentication within the extended enterprise for securing interoperable access • Prerequisite to authorization 	<ul style="list-style-type: none"> • Federal Bridge Certification Authority (FBCA) • HSPD12 (FIPS 201)
Connectivity	Establish the means to communicate.	<p>The Internet is generally available:</p> <p>For undeveloped or hostile environments:</p> <p>No connectivity</p>	"Big pipes" to bad places.	<ul style="list-style-type: none"> • Establishes the fundamental means to enable communications 	<ul style="list-style-type: none"> • Internet transport protocols

Table 4.1 – Abbreviated Federation Checklist

The authors took the concepts and guidance of previous chapters and consolidated them into an initial, abbreviated checklist that could be used by these federations for establishing their governance constructs.

This table captures the key conclusions of this paper. It synthesizes the core guidance for establishing governance within a federation over Principles, Architecture, Strategies, Needs and Investments in a focused way, and in a way that addresses the considerations (i.e., governance, culture, resources, policy, and technology) delineated within the DoD Information Sharing Strategy.

4.3. For Information Stewards:

Once an enterprise has made the decision to manage assets in common, including information assets, then actions by both the meta-governance and the stewards must be focused on the implementation of effective and continuation of effective stewardship. Again, the items under governance remain the same:

- Stewardship Principles
- Information Sharing Architecture
- The Services of Common Concern (e.g., directories, collaborative spaces, etc.) management by the steward
- Information Sharing Needs
- Investments and Priorities managed by the steward on behalf of the extended enterprise.

5. Recommendations for Follow-On Action:

The concepts in this paper represent an initial proposal regarding information sharing within federations in response to a specific request by an AFEI sponsor. The AFEI ISWG views this as a point of departure for future work.

Information sharing is a multifaceted problem, spanning all levels of the Extended Enterprise. Addressing these facets will require additional effort.

The AFEI ISWG therefore recommends a number of follow-on actions:

- **Establish pilot program(s) within DoD and the Extended Enterprise.** This paper delineates a number of actions that should be taken within the Extended Enterprise within extended enterprise, communities of interest and practice, and by information stewards. These concepts and strategies need to be proven. The AFEI ISWG recommends identifying mission/business problems requiring resolution, and then using the concepts and strategy to resolve them.
- **Investigate the feasibility of establishing a federal-level authority to act a “meta-governor” for the federal enterprise.** It may be appropriate to establish a central CIO organization to provide infrastructure and resources for an effective governance of data-/information assets and to assist the enterprise utilizing these assets. Further, the federal enterprise may need a regulatory organization to provide harmonized drafts of legislation, rules, regulations and guidelines for intellectual property rights, for governance, usage and for handling of sensitive information. This federal-level entity would be responsible for:
 - Information Sharing Principles and Information Sharing Investments across the federal enterprise.
 - Creating and managing a “utility” to maintain the capabilities managed in common at the federal level.
 - Assisting programs with identifying current data-/information resources (not information systems) and their status, costs, volume, lifecycle, legal and security constraints for sharing and map their users.
 - Assisting programs to evolve and migrate current data-/information resources to useable, secure and quality assured assets.. Make current data-/information



People, Process and Technology

assets more visible by including them into the general accounting and reporting procedures

- Set up oversight, key-values, budgets and other metrics to measure progress
- Initiate information sharing initiatives
- Set up the venues for stand up of CoIs and CoPs
- Be the “Fair Broker”

- **Begin the identification of specific, repeatable best practices for implementing these checklists and disseminate them with the Extended Enterprise:** One

consistent theme within the feedback that our colleagues have given us in response to their review can be summarized as follows: “Great analysis, but we need to make it ‘real world’. To be actionable, we need to be more specific and explicit in terms of the actions we want members of the federations to take.” Now that we have the basic dimensions defined, we need to take the next steps to flesh out this framework.



Appendix A - References

Reference [1] – *IT Governance, How IT Performers Manage IT Decisions for Superior Results*, Peter Weill and Jeanne W. Ross, 2004, Harvard Business Press, Boston MA

Reference [2] – IC-SOA Data Services Reference Architecture

Reference [3] - Federal Enterprise Architect Data Reference Model, Version 2.0

Reference [4] - Swedish Defense Information Vision (the blue book), Jarl S Magnusson, FMV, Version 1.0, Print 2, 2004

Appendix B - Definitions

Asset	Assets are economic entities that give rise to future economic benefit and are controlled by the entity as a result of past transaction or other events. (Wikipedia)
Collaboration	pattern of interaction where two or more parties are working together toward a common purpose
Culture	(Culture from the Latin cultura stemming from colere, meaning "to cultivate,") generally refers to patterns of human activity and the symbolic structures that give such activity significance. Different definitions of "culture" reflect different theoretical bases for understanding, or criteria for evaluating, human activity. In general, the term culture denotes the whole product of an individual, group or society of intelligent beings. It includes technology, art, science, as well as moral systems and the characteristic behaviors and habits of the selected intelligent entities. In particular, it has specific more detailed meanings in different domains of human activities. (Wikipedia)
Data	Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means. Any representation such as characters or analog quantities to which meaning is or might be assigned. (source: Joint Publication 1-02 of 12 April 2001 as amended through 09 Nov 2006)
Domains	A sphere of activity, concern, or function (source: The American Heritage® Dictionary).
Economics	Economics is the social science that studies the production, distribution, and consumption of goods and services. (Wikipedia)
Enterprise Integration	The vertical and horizontal alignment of plans, business processes, and information systems across organizational and functional boundaries to provide competitive advantage.
Federation	<ol style="list-style-type: none"> 1. Autonomous organizations operating under a common rule set to a common purpose. 2. Legally-binding framework to establish and maintain trust among autonomous organizations.



Definitions Continued

Governance	Governance is the practices of making decisions that define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes. Governance develops and manages consistent, cohesive policies, processes and decision-rights for a given area of responsibility. For example, managing at a corporate level might involve evolving policies on privacy, on internal investment, and on the use of data. (Wikipedia)
Information	<ol style="list-style-type: none">1. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms (source: DoD Directive 8000.1).2. Facts, data, or instructions in any medium or form.3. The meaning that a human assigns to data by means of the known conventions used in their representation (source: DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/).
Information Mobility	The dynamic availability of information. Information mobility is aided or impeded by culture, policy, governance, economics and resources and technology and infrastructure.
Information Sharing	Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.
Networks	A complex, interconnected group or system (source: The American Heritage® Dictionary). These networks include social, information technology, and communication networks.
Partner	DoD Information Sharing Strategy partner is an entity that takes part in an information sharing activity with DoD.
Policy	A policy is a deliberate plan of action to guide decisions and achieve rationale outcome(s). The term may apply to government, private sector organizations and groups, and individuals. (Wikipedia)
Risk Management	The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits (source: DoD Dictionary http://www.dtic.mil/doctrine/jel/doddict/)



Definitions Continued

Stakeholder	a DoD entity with a direct interest, involvement, and investment in DoD information sharing.
Technology	Technology can be most broadly defined as the entities, both material and immaterial, created by the application of mental and physical effort in order to achieve some value. Infrastructure is generally a set of interconnected structural elements that provide the framework supporting an entire structure. (Wikipedia)