# Assured Information Sharing Life Cycle

**Tim Finin, Anupam Joshi, Hillol Kargupta, Yelena Yesha, Joel Sachs**
**The University of Maryland, Baltimore County**

**Elisa Bertino, Ninghui Li, Chris Clifton, Gene Spafford**
**Purdue University**

**Bhavani Thuraisingham, Murat Kantarcioglu, Alain Bensoussan, Nathan Berg, Latifur Khan**
**The University of Texas at Dallas**

**Jiawei Han, ChengXiang Zhai**
**The University of Illinois, Urbana Champaign**

**Ravi Sandhu, Shouhuai Xu, Jim Massaro**
**The University of Texas at San Antonio**

**Lada Adamic**
**The University of Michigan**

***Abstract*—**This paper describes our approach to assured information sharing. The research is being carried out under a MURI (Multiuniversity Research Initiative) project funded by the Air Force Office of Scientific Research (AFOSR). The main objective of our project is: *define, design* and *develop* an Assured Information Sharing Lifecycle (AISL) that realizes the DoD's information sharing value chain. In this paper we describe the problem faced by the Department of Defense and our solution to developing an AISL System.

## I. Introduction

Daniel Wolfe (formerly of the NSA) defined assured information sharing (AIS) as a framework that "provides the ability to dynamically and securely share information at multiple classification levels among U.S., allied and coalition forces." The DoD's vision for AIS is to "deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment" In our current project on AIS, our objective is to help achieve this vision by defining an AIS lifecycle and developing a framework to realize it.

The main objective of our project is: *define, design* and *develop* an Assured Information Sharing Lifecycle that realizes the DoD's information sharing value chain. To achieve this objective we will develop tools and techniques including the following: (i) a comprehensive policy framework that provides support to specify and reason with a variety of policies including confidentiality, accountability and trust, (ii) an event-based secure service oriented architecture that will support the services for assured information sharing, (iii) a security infrastructure that will provide the services needed to enforce the policies for life cycle oriented applications and management, (iv) techniques to exploit social networks to forge information mobility, (v) approaches for assured information integration, analysis and quality, (vi) tools for assured behavior-based incentivized information sharing.

## II. The Problem

In order to fight the global war on terror the DoD, federal agencies, coalition partners and first responders, among others have to proactively share information and make effective decisions. Yet in doing so, one must protect the confidentiality of sensitive information and appropriately respect the privacy of individuals. Traditional security policies are often based on the concept of "need to know" and are typified by predefined and often rigid specifications of which principals and roles are pre-authorized to access what information. One of the recommendations of the 9/11 commission (Markle 2003) was to find ways to move from this traditional perspective toward one that emphasizes the "need to share". Our research to address the

978-1-4244-4173-0/09/$25.00 ©2009 IEEE

above problem will be guided by (i) DoD's information sharing strategy and (ii) scenarios that are relevant to information sharing needs of the DoD and other Government agencies. Information includes contextual data, metadata, and descriptions of architectures, resources, policies, processes and strategies.

In May 2007 the DoD CIO published a document (DoD 2007) that articulated DoD's Information Sharing strategy. The vision for information sharing is to "develop the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment." To achieve this vision, the DoD has formulated the following four goals: (i) "Promote, encourage and incentivize sharing" (ii) "Achieve an extended enterprise" (iii) "Strengthen the agility in order to accommodate unanticipated partners and events" and (iv) "Ensure trust across organizations." DoD has stated that the four information sharing goals will be realized through five implementation strategies that we reference and address in this proposal.

Our initial scenario pertains to the Distributed Common Ground System (DCGS). To ensure the horizontal integration of joint intelligence, surveillance and reconnaissance (ISR) sensor platforms for improving time critical targeting, the DoD is developing DCGS as a global intelligence-sharing network, based on network centric enterprise service oriented architecture. While the Air Force is developing DCGS (with Raytheon Corporation as the prime contractor), the Navy is developing its version called DCGS-N and the Army is developing its version called DCGS-A. The three organizations must share information for combat operations via DCGS as well as with foreign intelligence services (NRC 2006). We will show how our research can enable and enhance this system, and also explore other scenarios with our collaborators.

## III. AISL

AISL consists of three major phases shown in Figure 3-1: (1) information discovery and advertising, (2) information acquisition, release and integration and (3) information usage and control. These phases will realize the information sharing value chain of (DoD 2007). During the *discovery phase* parties advertise the information they own and search for relevant information. Each party in the *information landscape* may thus play two main roles: information provider and information consumer. Information discovery and advertising entail several issues: determining what and to whom to advertise, supporting selective advertising, ensuring confidentiality and verifying integrity, and determining incentives for information sharing. Information *acquisition, release and integration* entails several issues: determining what information to release and to whom, verifying the need for the information, evaluating the risk and benefits in acquiring/releasing the information, and stating and evaluating obligations derived from information acquisition and release. In the *usage and control* phase, a key requirement is that information providers maintain "an awareness of where and how this information is used" (DoD 2007). This entails addressing several issues: controlling how information is used once it is released, joint administration, access control and accountability, investigating confidentiality and integrity breaches, and assessing the benefits derived from its use.

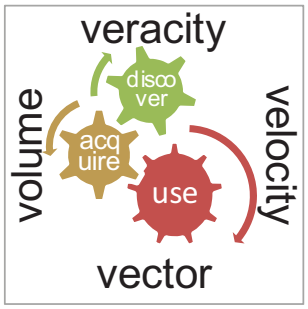
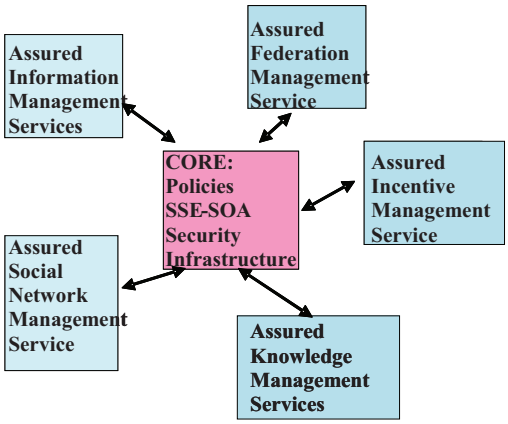



**Figure 1. The Assured Information Sharing Lifecycle has three major components**

The AISL is a concrete embodiment of *the notion of assured information sharing value chain* in that it provides a set of services, tools, and processes collectively able to *securely* assemble the right combination of information sources and instantly being able to *securely* communicate, coordinate, and respond appropriately to the situation at hand. As such the AISL is highly dynamic and can rapidly react to situations but at the same time provides security guarantees. The above three phases are

executed multiple times by several processes and for different classes of information. Figure 2 illustrates the various modules that will implement AISL. The glue consists of policies, secure semantic event-based service oriented architecture (SSE-SOA) that supports web services, and a security infrastructure that supports the enforcement of the policies. The high level web services include assured information management, assured knowledge management, assured social networking, assured incentive management and assured federation management.




**Figur 2 Assured Information Sharing Lifecycle System**

Our goal is to *get the right information to the decision maker so that he/she can make decisions in the midst of uncertain and unanticipated situations.* We are developing tools and techniques to assess and/or quickly re-validate the information to be used for decision making, as well as to enhance the information about *origin*, through the use of accountability processes. By using our tools, the decision maker can determine the origin of the information. Such awareness may prompt for additional fast validation of information, leading to rapid search for other information that can confirm or invalidate the initial information. The AISL is dynamic and supported by information quality and provenance techniques in all its phases. Our future papers will discuss the details of AISL.

**ACKNOWLEDGEMENTS:** This work is sponsored by the Air Force Office of Scientific Research under an FY 2008 MURI Project on Assured Information Sharing. We thank Dr. Robert Herklotz of AFOSR for his support.

## REFERENCES

(DoD, 2007) DoD (Department of Defense) Information Sharing Strategy. May 2007, available at: http://www.defenselink.mil/cio-nii/docs/InfoSharingStrategy.pdf.

(Markle, 2007) Markle Report on Assured Information Sharing, The Markle Foundation, 2003