

WIS³



WORKSHOP ON INFORMATION SHARING AND SAFEGUARDING STANDARDS FRAMING THE ASK OF THE BREAKOUT GROUPS

Welcome to the Workshop on Information Sharing and Safeguard Standards, aka “Standards Palooza” which builds upon last year’s event when industry and government came together to chart a way forward for standards in support of the Information Sharing Environment.

At last year’s event four major themes emerged about how industry and government could work together to advance the ISE:

- Immediately leverage existing standards
- Prohibit “data lock down”
- Drive standards
- Build community

For this year’s event, we want to continue the energetic dialogue to identify short- and long-term activities to enable whole-of-government information sharing and safeguarding through standards. In evaluating which standards to use internally for information sharing and shared information services, U.S. government departments have primarily focused internally on their standards efforts resulting in:

- Parallel but unconnected efforts across departments
- Unmet realization of responsible information sharing across departments
- Standards gaps and duplicity
- A lack of clear signals to industry as to which government standards are important

The bottom-line: When it comes to responsible information sharing, **it’s not that there is a lack of standards – it’s that there are too many different standards** being used across government. If the vision of whole-of-government responsible information sharing is to be achieved, different departments and agencies will need to reach consensus regarding what standards, profiles, and frameworks to use.

To help to address these challenges, the WIS³ Breakout Groups should identify activities industry and government could take together “across the chasm” and answer:

Using standards – how do we achieve the “whole of government” vision where any authorized person, with the right legal authority, can find & access securely information at the right time, appropriate to his or her mission activities?

With this key question, four cross-cutting questions span across each of the breakout groups:

- **How do we identify the processes, relationships, data structures & attributes associated with the information sources resident in different agencies & enterprise architectures, and record those models for sharing?**
- **How do we implement proper access controls and associate attributes with the authorized persons overseen by different departments?**
- **How do we abstract the role of distributed information stewardship, exercised by different community members, from the physical role of information storage and services, while integrating those different communities?**
- **How do we translate business requirements into technological approaches to automate information access based on data attributes, access controls and attributes, and applicable responsible information policies, especially when the technological underpinnings keep changing?**

The morning sessions of the WIS³ Breakout Groups should provide context and future-focused vision of specific standards-based responsible information sharing efforts. The goal is to evaluate common questions about the future to later be discussed in the afternoon sessions. The afternoon sessions should consider both the four cross-cutting questions that span across each breakout group, as well as specific questions associated with each group, to include:

1	Supporting Standardized Information Exchanges Across Government Standardized information exchange models that enable interoperable information sharing. (Angle Room)
	<ul style="list-style-type: none"> 1.1. What is the future of NIEM 3.0 and how does it scale to include additional partners, IC, DoD, et al.? 1.2. How do we include advanced Geospatial Capabilities in NIEM, given NIEM is messaging-agnostic? 1.3. How do we go beyond IEPDs to enable Discovery, is DDMS a way-forward with NIEM?
2	Identity and Access Management Across Government Authenticating and authorizing ISE users to access information sharing systems and data. (Vista Room)
	<ul style="list-style-type: none"> 2.1. What infrastructure does FICAM need to identify and monitor user access behaviors across gov't? 2.2. What infrastructure does gov't need to govern and use attributes for access control across gov't? 2.3. How can we do trust federating across gov't to include advancing GFIPM as an industry standard?
3	Federated Information Sharing Frameworks and Services Messaging frameworks and services that can operate across agencies. (Academy Hall)
	<ul style="list-style-type: none"> 3.1. How do we address the message header interoperability across service frameworks? 3.2. What are the APIs departments need to expose to make available services across government? 3.3. How do we encourage provision, reuse, and reimbursement for share services across government?
4	Translation of Business Requirements into Solutions Translating business requirements to technical architectures to automate information sharing. (Academy Hall)
	<ul style="list-style-type: none"> 4.1. How do we scale privacy policy automation across government via open standards? 4.2. How do we scale standards interoperability across government departments, is DNDO a model? 4.3. How do we scale translation of business requirements to technical requirements, is UPDM a model?

The WIS³ Breakout Groups will provide a report at the end of the day to Senior Leaders in Government, including identification of short- and long-term activities both industry and government could take to enable whole-of-government information sharing and safeguarding through standards.

We sincerely hope this Workshop represents the continuance of an on-going set of energetic activities and dialogue to accelerate delivery of the ISE. We welcome comments on the ISE website and blogs, www.ise.gov and identified opportunities to continue the momentum in industry and government forums.