Potential Use of Federal Data Standards

MOISA Year Two reviewed a set of emerging Federal data standards as listed under the Project Interoperability website, developed by the Program Manager of the Information Sharing Environment (PM-ISE) for potential use in improving identification and information management to enhance mission goals.[1]

> "Information interoperability is the ability to transfer and use information in a consistent, efficient way across multiple organizations and IT systems to accomplish operational missions. From a technical perspective, interoperability is developed through the consistent application of design principles and design standards to address a specific mission problem."[2] – Project Interoperability website

One of MOISA's goals is to facilitate information sharing among various organization with different missions and resources. The two main components of information sharing are building trust-based relationships to encourage information sharing and developing the technical capabilities to efficiently and securely share agreed upon information. Much of MOISA's work through its second year has been focused on the former. MOISA's third year will expand to help willing partners facilitate automated information exchange.

PM-ISE's Project Interoperability draw from ten main information sharing tools to facilitate timely and responsible information sharing throughout the Puget Sound region. These tools are described below:

Identity and Access Management (IdAM)[3]: IdAM is a diverse portfolio of technical systems, policies and processes that create, define, and govern the use and safeguarding of identity management, authentication, and authorization, as well as managing the relationship between an entity and the resources to which access is needed.[4] Implementation of IdAM protocols can provide an organization an auditable means of ensuring that access to its sensitive information and facilities is only granted to the appropriate individuals.

The ISE Common Profile Framework Description[5]: A "Common Profile" documents a standard method of achieving a desired outcome. It provides a template for consistently documenting the contents of a profile within and across organizations. Standards are often available online in configuration-managed registries for expanded use among multiple agencies. Profiles developed by an organization or working group are often published in a Profile Registry, which allows for sharing of the common profile within an expanded group or with similar groups attempting to create similar information sharing protocols. As such, Common Profiles developed in conjunction with a small group of actors in the Puget Sound security community could be shared locally to expand the group, or nationally to enable other regions to benefit from developments in the Puget Sound region.

---

[1] Project Interoperability website http://project-interoperability.github.io/ accessed 7/17/15.
[2] Ibid.
[3] http://project-interoperability.github.io/idam/ accessed 7/22/15.
[4] http://www.disa.mil/Initiatives/Identity-Access-Mgmt accessed 7/24/15.
[5] http://ise.gov/sites/default/files/Common_Profile_Framework_v2_2015.pdf accessed 7/17/15.

Springboard[6]: Springboard is a service operated by the non-profit Integrated Justice Information Systems (IJIS), which evaluates and certifies program compliance with information sharing standards. The implementation of Springboard in July 2012 provided the first means to verify vendor and developers' claims of compliance with information sharing standards. Springboard currently certifies compliance in justice, public safety, and homeland security communities.[7]

Architecture Alignment[8]: As documented by MOISA, regional maritime safety and security communities are comprised of actors representing many functional and organizational communities, using a variety of ISE architecture frameworks. Architecture Alignment is the process needed to create interoperability among these architectures. Project Interoperability's efforts are not intended to drive convergence of the frameworks, but to assist alignment among the frameworks from an ISE interoperability perspective.

Maturity Model[9]: The maturity model provides a means of evaluating mission reference architecture and interoperability architecture artifacts. The ISE maturity model is broken down by the common approach (CA) domains in the Federal Enterprise Architecture (FEAF): Business, Data, Applications and Services, Technical, and Performance.[10] Each level of interoperability is categorized in one of five levels: ad hoc, repeatable, enhanced, managed, and optimized. The goal is not necessarily to reach the 'optimized' level for each domain. Individual organizational needs will create requirements for the maturity level of each category.

Reference Architecture Template[11]: "Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions."[12] Reference architecture (RA) templates assist in the development of reference architecture tools to support interoperability. For each of the CA domains in the FEAF, the templates guide relevant interoperability requirements and artifacts to be incorporated for interoperability. The template details interoperability goals in each of the domains, as well as instructions for template usage. Benefits of a reference architecture framework include:

- A common language for the various stakeholders
- Consistency of implementation of technology to solve problems
- Validation of solutions against proven Reference Architectures
- Adherence to common standards, specifications, and patterns[13]

Attribute Exchange[14]: Attribute exchange is the ability to pass information related to a user's access-control between two or more organizations, either automatically or on demand. Attribute based access

---

[6] http://www.ise.gov/blog/carrie-boyle/prove-your-interoperability-and-standards-compliance-ijis-springboard accessed 7/17/15.

[7] https://ijis.site-ym.com/?page=Springboard accessed 7/17/15.

[8] http://project-interoperability.github.io/architecture-alignments/ accessed 7/20/15.

[9] http://project-interoperability.github.io/maturity-model/ accessed 7/21/15.

[10] https://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf accessed 7/21/15.

[11] http://project-interoperability.github.io/ref-arch-template/ accessed 7/21/15.

[12] http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf accessed 7/22/15.

[13] Ibid.

[14] http://project-interoperability.github.io/attribute-exchange/ accessed 7/22/15.

control (ABAC) is a method of providing access based on the evaluation of a user's attributes. Some view ABAC to be an advance over previous methods of granting access, such as access-control lists or role-based access control (RBAC), because they view it to be less cumbersome to manage.[15]

Exchange Patterns[16]: Exchange patterns are repeatable sets of tasks that help accomplish a commonly occurring need for information or data exchange between and among information sharing partners. Exchange patterns describe core functions within an information sharing activity, and they are documented along with interoperability technical standards and services requirements as part of an information exchange specification.

National Information Exchange Model (NIEM)[17]: NIEM helps Communities of Interest (COIs) to develop on-demand information exchange protocols to allow for information sharing among new and existing partners. COIs work together to create Information Exchange Package Documentation (IEPD), which defines message types, structures, context, and meaning. By developing a set of protocols to be used among the community, members save resources by obviating the need to negotiate and implement individual, bilateral agreements. New or nontraditional partners can quickly join in information sharing with members of a NIEM COI by using established IEPD without the need to set up new information exchange protocols.

ISE Standards Specifications Framework[18]: The Standards Specifications Framework provides a structure to develop the tools necessary to identify and normalize standards to enable interoperability. The Framework describes interoperable information exchange attributes, including standardized requirements and definitions. Although specific processes and requirements vary, standardizing information sharing exchanges into patterns enables interoperability and supports future growth across disparate jurisdictions.

Pending funding, the third year of MOISA research will build on this initial analysis to analyze how interoperability tools and concepts are useful and applicable to mission accomplishment, discuss why some tools may not be useful, and recommend strategies to improve tool design, usability, and outreach.

---

[15] http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf page vii, accessed 7/22/15.
[16] http://project-interoperability.github.io/exchange-patterns/ accessed 7/22/15.
[17] http://project-interoperability.github.io/niem/ accessed 7/22/15.
[18] http://project-interoperability.github.io/standards-specifications/ accessed 7/23/15.