INFORMATION SHARING ENVIRONMENT (ISE)

SENSITIVE BUT UNCLASSIFIED (SBU) TECHNICAL ADVISORY COMMITTEE (STAC) NATIONAL INTEROPERABLE SBU FEDERATION CONCEPT OF OPERATION (CONOP)

Prepared by the
Sensitive but Unclassified Technical Advisory Committee and the Office of the Program Manager for the Information Sharing Environment

November 15, 2016

This page intentionally blank.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Terrorism and public safety related information that is processed by local, state, federal, tribal, and territorial entities often constitutes SBU information. Outside the federal government, almost all information is shared at the unclassified level. The "National Strategy for Information Sharing and Safeguarding" (NSISS), December 2012, stresses the critical role of SBU information sharing in efforts to strengthen national security and public safety. One of the critical challenges, as highlighted by the NSISS, is "A lack of network interoperability that creates barriers across departments and agencies and missions."

The Sensitive But Unclassified Technical Advisory Committee (STAC), a subsidiary group of the Information Sharing Council (ISC), was established to support ISC duties pertaining to the sharing of national security, public safety and terrorism information among SBU environments. The STAC mission is to promote and advance responsible sharing of timely, accurate, and comprehensive SBU information by federal, state, local, and tribal partner agencies and stakeholders across the full spectrum and scope of their respective missions, under their own authorities, to achieve mission effectiveness.

There have been many lessons learned by existing STAC members that each work within their own missions and under their own authorities. This paper outlines the operating concepts necessary to connect the entire SBU landscape and drive successful implementation of SBU information sharing in: Access, Discovery/Search, and Shared Services.

1 Background and General Reference Information

Senator Richard Shelby, vice-chairman of the Senate Select Committee on Intelligence, in his investigative December 2002 report on the events of September 11th, 2001 noted that prior to 9/11: "the most fundamental problem . . . is our Intelligence Community's inability to connect the dots."

Since then "connect the dots" has become a mantra for information sharing experts and there have been countless calls for a multifaceted system of networks to sift through huge volumes of terrorism related data. Uncovering information critical to the Nation's law enforcement and homeland security professionals requires consideration of data protected at sensitive but unclassified and controlled unclassified information (SBU/CUI) levels.

The following comments from two senior leaders reinforce the importance of cooperation and connecting our SBU data systems together. Former Coast Guard Chief Knowledge Officer, Dr. Nat Heiner offered up a reasonable solution. He observed that: "In order to first connect the dots, you need to first connect the people." In her remarks at the Technologies for Public Safety in Critical Incident Response Conference and Exposition on September 27, 2004 in New Orleans, LA the Honorable Deborah J. Daniels Assistant U.S. Attorney General, Office of Justice Programs, said: "We all understand that we need to interlink, as a single backbone for information sharing, HSIN, RISS, LEO, JRIES (Joint Regional Information Exchange System), and other systems, to reduce confusion and increase speedy access to information. Yet, a patchwork of information sharing systems, networks, and portals still exist among Federal, State, local, and tribal departments, agencies, in cooperation with private sector organizations.

The terrorism information that is processed by local, state, federal, tribal, and territorial entities often constitutes SBU information. The 2012 National Strategy for Information Sharing and Safeguarding (NSISS) stressed the critical role of SBU information sharing in efforts to strengthen national security and public safety. One of the critical challenges, as highlighted in the Strategy is: "A lack of network interoperability that creates barriers across departments and agencies and missions."

Absent a capability to seamlessly share this information efficiently and effectively across disparate, sequestered information technology systems represents a continuing risk to national security.

To fix this problem, the Program Manager – Information Sharing Environment (PM-ISE) tasked the Sensitive but Unclassified Technical Advisory Committee (STAC)[1] to describe these fundamental operating concepts of the National Interoperable SBU Federation (hereafter referred to as the "Federation").

The Business Process working Group (BPWG), a predecessor of the STAC, was chartered to, among other things, assess, prioritize, and map business processes critical to the distribution of

[1] The STAC is a subsidiary group of the Information Sharing Council established in Section 1016(g) of the Intelligence Reform and Terrorism Prevention Act of 2004 and in Executive Order 13388 of October 25, 2005 ("Further Strengthening the Sharing of Terrorism Information to Protect Americans").See STAC Charter https://www.ise.gov/resources/document-library/charter-sensitive-unclassified-sbu-technical-advisory-committee-stac

terrorism-related information and creation of a federated ISE for that purpose. The BPWG documented user requirements and distilled them down the following essential components:

- Access[2]: "I want to log in one place, one time and get to what I need, wherever it is --No Wrong Door";
- Discovery and Search[3]: "I want to launch one search and get everything that I need/want back";
- Shared Services[4]: "What tools and services are out there to help me do my job?"

The STAC, building on the work of the BPWG and the Sensitive But Unclassified Working Group, has been tasked with the ambitious goal of bringing together people and systems to meet its mandate of advancing SBU information sharing services by enabling stakeholders to responsibly share timely, accurate, and compressive law enforcement, public safety, and homeland security information.

This paper articulates the common operating policies, processes and procedures necessary to establish the National Interoperable SBU Federation[5] as an integrated set of solutions to address the existing SBU information sharing gaps in Access, Discovery/Search, and Shared Services.

2 Operational Concepts to Create a National Interoperable SBU Federation

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 point of view, interoperability is developed through the consistent application of design principles and standards to address a specific mission problem. Administrative preconditions to interoperability, such as policies and procedures, must be in place to exchange and safeguard the information.

Information interoperability is important because it increases timely, responsible information sharing, can reduce costs and redundancy, and use best practices. These are all things that enhance decision making for government leaders, industry, and citizens.

The STAC recommends that three operating principles form the basis of ongoing Federation activity:

1. ***The Federation will use a common set of references and standards.*** PM-ISE has been working with the Standards Coordinating Council (SCC) – a government-industry

[2] Access: Process used to grant an individual access to information and associated resources of ISE member communities based on verification of the individual's identity (Identity Management), security credentials and assigned mission roles. Process must ensure security and currency of credentialing and role data. It also protects personal identify information where applicable

[3] Discovery and Search: Allow ISE participants to conduct queries of disparate terrorism-related information; support ISE participants' ability to discover data from sources a participant may otherwise not know exists.

[4] Shared Services: Assists in locating people, organizations, information and services related to or supportive of the counterterrorism mission.

[5] The National Interoperable SBU Federation (the Federation) is a collective of network and system providers who agree upon standards of operation that enable a flexible yet secure SBU Information Sharing Environment. A federation (no caps) refers to a collection of systems and networks that adheres to a set of operating principles and standards to achieve interoperability.

consortium -- to furnish an integrated suite of technical and managerial resources and expertise to promote the development of ISEs between federal, state, local, tribal, and private sector mission partners at the domestic nexus of national security and public safety. Project Interoperability 2.0 (PI 2.0) organizes delivery of models, standards, guidance, training, and other framework artifacts to help establish ISEs and make them better – i.e., more standardized, scalable, and equipped with best-fit technology. The Federation has aligned their efforts with an important component of PI 2.0, the Information Sharing and Safeguarding (IS&S) Core Interoperability Framework (ICIF). The ICIF enables the standardized implementation of a suite of hardware and software that can assure wide-scale interoperability and trust within an ISE. The ICIF consists of a collection of pre-existing, externally-published and -vetted technical and policy sources (including NIST SP 800-53, NIST SP 800-63, the FBI CJIS Security Policy, FICAM, NIEM, SAML, OpenID Connect, GML, and others).

2. ***Data should be available to Federation users without unnecessary restriction; responsibility for access rules lies with the data owner.*** Producers of SBU data must remain accountable for the management, maintenance and administration of access to their information products while the consumer experiences maximum flexibility in using information acquired through the Federation. The discovery and search tools available within the Federation must remain responsibly available to the consumer without unnecessary restriction. The more the Federation unnecessarily restricts the SBU environment, the more likelihood it will ultimately fail those with a mission need.

3. ***Trust among Federation participants will be assured through the use of digital assertions.*** An Assertion-Based Architecture (ABA) is a technical framework that enables the wide-scale use of digital assertions to convey trusted statements (assertions) about the compliance of ISE participants with rules derived from the external sources. The ABA acknowledges the inherent heterogeneity that exists among ISE stakeholders with respect to implementation, conformance, and compliance with policies. The ABA enables those stakeholders to demonstrate alignment with appropriate parts of the body of rules in a format that is componentized and reusable, and allows data owners to specify the components needed in order for access to be granted to any particular data.

3 Approach to Simple and Secure Access Control

Federation members will promote a “no wrong door” approach for access to the Federation. No wrong door implies that a user in the Federation with the proper and asserted credentials will be able to access information and data within the Federation. Why is this important? “We don’t want the user to get hung up on what network is what. The user needs to be able to access the tools they need to support their mission”.[6]

The federated user’s access will be determined by applicable rules, regulations, policy, auditing, monitoring, and security controls set down by the data’s steward regardless of the user’s initial starting point. While federations, including Single Sign-On (SSO), alter the risks associated with identity management, every user of a federation SSO enabled platform is heavily vetted before

[6] https://www.ise.gov/blog/ise-bloggers/live-nfca-annual-training-event-no-wrong-door-sbu-information-sharing

they can gain access to their home system. Periodic re-vetting of users is also necessary to ensure that the credentials remain trustworthy over time.

Federation members agree to exchange authenticated identity information along with approved authorization attributes – moving towards a federated identity model. This effort promotes trust among current and future federation members through a framework built on transparency, autonomy, sharing, and assurance for user identity and access to information. Standardizing these attributes allows new and existing SBU organizations to quickly access information resources held by other federation members.

In addition to using an approved set of attributes, the Federation will use a standardized attribute assertion (SAML protocol message) to exchange attribute names and values between SBU identity and access management (IdAM) systems. Standardized attribute assertions enable all participating members to enjoy quicker acceptance from, and provisioning of services by, partner systems**.**

Streamlined access to information resources across organizations strengthens the Federation and enhances mission effectiveness. Members of the Federation not only safeguard data through strong identity management practices, while gaining access to the services which the other members of the Federation choose to expose. Once part of the Federation, the need for multiple usernames and passwords, manual logins, and manual account processing is reduced or eliminated.

4 Approach to Intelligence Information Discovery and Search

Discovery and search is a logical sequence for finding and collecting restricted data on intelligence systems. Discovery answers the question: "what information is available, relevant to a specific intelligence topic." Discovery provides non-sensitive indexed metadata that analysts use to narrow their search, minimizing the amount of sensitive information retrieved by search tools. In the Federation, the goal of discovery, federated search and retrieval functionality is to provide authorized SBU system users the ability to conduct omnibus search and retrieval of all federated information sources. For example, a user is logged into their local SBU system and is interested in information on a specific type of terrorism incident. The user navigates to a search interface and submits a query. The user receives not only results from local resources, but also results from other partner SBU systems.

For this to happen, each SBU system must expose data to the federation using a standards-based approach consistent with the three (3) content search methods. The major components include (and each are expanded on in the table below):

1) A federated search

2) An enterprise catalog

3) A centralized crawler software product/solution

Use of administrator configured search options permits agencies to specify how their data sources are indexed and labeled so sensitive content is protected while giving users direct references to data owners who can readily share restricted information once need to know is established.

Table 1: Standard Search Methods

Standard Search Method	Description
Federated Search	A real-time, simultaneous search of multiple resource collections that may reside on many separate domains. Federated Search utilizes a service to accept a query request, broadcast it out to a number of providers, each provider can optionally trim the results based on the user's attributes, and then aggregates the results into a combined set for the consumers.
Centralized Search	Operates by creating a central index of content obtained by crawling web sites and following web feeds. Search queries are then executed against the index.
Enterprise Metadata Catalog	A central catalog of discovery metadata organized into collections. The Enterprise Metadata Catalog searching mechanism supports precise criteria such as geospatial and temporal parameters as well as full-text search. The Defense Discoverable Metadata Specification (DDMS) is an example of an appropriate metadata tagging standard for the contents of an Enterprise Metadata Catalog.

Since a patchwork of SBU information systems, networks, and portals exist, harmonizing existing search functionality together into enterprise wide capability is not a trivial effort and is best met using a "lead partner" approach. The lead partner works to gain consensus among the participating system partners on a plan to design their federated capability and then champion implementation within their organization. The lead partner will also work to ensure partner systems:

- Identify and categorize their data resources and specify the subset they intend to provide to the search capability.
- Expose their specified data resources to federated search implementation using applicable standards.
- Test and validate the ability to search, discover, and retrieve data.

The Standards Coordinating Council published IS&S Playbook[7] provides guidance to law enforcement, public safety, intelligence, homeland security, and many other mission partners who want to jointly address IS&S challenges, develop communities of practice, and otherwise advance the IS&S mission. The book contains 15 'plays' which together constitute a step-by-step

[7] http://www.standardscoordination.org/iss-playbook

guide to managing the build-out or upgrade of an ISE. The Playbook is useful both to experienced and novice managers of cross-agency technical projects, and maps the models, standards, checklists, and other resources offered by Project Interoperability 2.0 to the capability acquisition phase(s) they most directly contribute to. The current version of the Playbook can be viewed and downloaded at: www.standardscoordination.org.

A forthcoming IS&S Technical Assistance Directory will provide online pointers not only to the various PI 2.0 products, but to subject matter experts (SMEs), signature authorities, organizational homepages, information technology (IT) vendors, GFE, applicable law and regulations, and many other resources that COIs can leverage to obtain ISE-related technical assistance and training services.

5 Approach to Shared Services

A key component of the Federation is what the IRTPA refers to as "electronic directory services or the functional equivalent."[8] Based in part on a concept articulated by the Markle Foundation's Task Force on National Security in the Information Age, electronic directory services will help authorized participants, including analysts, operators, responders, planners, and policy makers, to locate information, organizations, services, and personnel in support of their respective requirements.

Today any number substantive electronic directory services exist within several of the individual communities that will make up the Federation, although they are most often used to locate people rather than information. To build an electronic directory service for all users requiring terrorism information, however, we need to leverage what exists today and introduce new capabilities to build upon and harmonize these systems toward our end goal.

The following capabilities requested by SBU system users represent specific capability objectives under the umbrella of shared services:

- The capability to search all participating SBU systems for relevant content, people and services accessible and searchable through an integrated, federated process that assures appropriate access procedures, rules, and qualifying data are included within the SAML message;
- The capability for user organizations to register (add) people to access lists and allow them to opt-out if needed; and,
- The capability to modify profile information on individual users and/or remove them from a directory.
- The capability to register (add) a service; and,
- The capability to enable administrator to modify or remove a service from searchable directories when they present security or operational risks.

[8] In this case the functional equivalent is "shared services".

Directory services are but one example of a service that could be shared by federation partners. However, other shared services could be made available to further advance information sharing among federation partners.

Among many other sharable resources, Project Interoperability offers architecture alignment guidelines and the IS&S Common Profile which provides guidance on how stakeholders' diverse information architectures can be characterized, rendered comparable to one another, and ultimately aligned with different aspect of the ICIF without causing architectural issues or breaking any key component. Such alignment is prerequisite to an organization's ability to either offer or ingest shared services, and to efficiently share information within the context of an ISE.

6 Governance

Governance, in its purest form, describes the structures and decision making processes that allow a group of people to conduct affairs with accountability. In the Federation, day to day governance occurs at the system level and is exercised by the organizations that fund the operations. Responsibility for oversight of STAC members regarding joint decisions and standards is established in the STAC charter. As the SBU Federation evolves, the STAC or another oversight body must exist to ensure adherence to SBU information sharing goals and objectives.

Project Interoperability 2.0 supports governance by making available a Common Lexicon that aligns agencies' information architectures and acquisition projects on a shared set of IS&S-specific terminology approved by recognized standards organizations. PI 2.0 also offers resources to assist ISE stakeholders in determining the scope and high-level operational requirements applicable to their ISE development efforts. One such resource, the IS&S Performance Scenario for the SBU Domain, exists primarily to guide engineering choices and processes, and secondarily to help convince sponsors and partners of the value of the proposed SBU ISE build/enhancement. Similarly, the ICIF Capability Model illustrates levels of mission capability for each of several key aspects of information sharing, thus allowing senior managers to tell at a glance "where they are" with respect to information sharing, as well as "where [to what capability level] they wish to go".