SAVIN TECHNOLOGY STANDARDS

SAVIN systems have a vital role in the provision of accurate, timely, and relevant information to victims. Additionally, as SAVIN systems become a more integral function of the Criminal Justice Information System (CJIS) enterprise, the data contained in these systems can become part of a more comprehensive compilation of information available to victims and others within the criminal justice system.

Access to this crucial offender information is possible through the consistent use of SAVIN technology solutions. Information sharing for SAVIN includes implementing:

- ☐ Key policies (such as those related to privacy/security)
- ☐ Relevant national information sharing standards as recommended by DOJ’s Global Justice Information Sharing Initiative (Global), such as Global Reference Architecture (GRA), National Data Exchange Model (NIEM), and Global Federated Identity and Privilege Management (GFIPM)
- ☐ SAVIN IEPD/Service Specifications and other currently available technologies that support SAVIN business processes

Business Processes Related to Victim Information and Notification Technology

Statutory requirements to notify victims of specific events in the criminal justice process exist in all states and at the Federal level in the U.S. Most criminal justice agencies are required to provide notification to crime victims, witnesses, and interested parties. Notifications can be automated and provided through various methods (telephone, email, text/SMS, TTY/TDD, and/or mail) and add complexity to the overall SAVIN business process.

Victim information and notification systems do not control or determine the timeliness of the notification message to the victim. The delivery of notification is determined by the timely entry of data into the originating system and the delivery mechanism used. The notification system is, however, responsible for the processing and delivery of a notification to the victim(s) and other registered users. Audited communication channels must show the origin of the message, the means of delivery and the date and time that the system provided the message to the victim or interested party.

System/Data Administration/Management

To support SAVIN business processes, the overall SAVIN architecture should support the ability to share data among multiple data sources. The solution must accept data from the participating agencies’ existing JMS, OMS, and CMS systems and be able to process the respective data to provide information and notifications. In no way should the SAVIN solution dictate a standard for a JMS, OMS, or CMS system. An Enterprise Architecture (EA) model should be considered in the system and data management which aligns with the overall program strategy. An EA model as it relates to the management of systems and data falls into multiple layers as shown below in *Figure 1*.

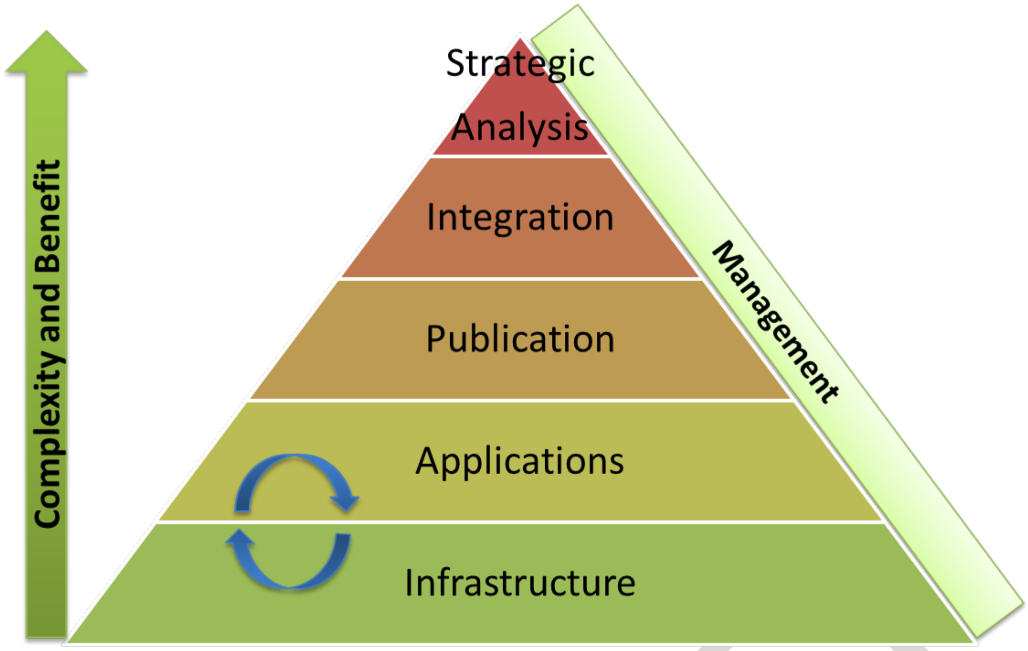

Figure 1

Each layer builds on the layer below in the pyramid. The complexity of the technology environment, as well as the business value, increases progressively in each layer toward the top of the pyramid. Early identification of the potential changes in the different layers through the planning process provides input for tactical project planning and helps manage the overall rate of change in the environment. Each SAVIN Program Managers should understand the value of this pyramid and work with his or her IT staff to ensure that they have complete understanding of what makes up each layer and how it supports the overall program strategy.

The following details describe each of the pyramid's layers.

Infrastructure Layer

Infrastructure components provide technology solutions that deliver, secure, and run business systems. Examples of these infrastructure components include:

□ Firewall systems that isolate system resources from unauthorized systems
□ Intrusion-detection mechanisms within the network environment
□ Certificate or token systems that provide message surety to users and systems outside of the secured environment
□ Backup systems that provide information- and system-recovery capabilities
□ Data center design that provides consistent support and operational service to the agency users
□ Workstation equipment sufficient to support the agency business applications
□ Network infrastructure that provides connectivity to internal and external agencies

These infrastructure components provide the foundation upon which the business applications layer operates. Many components within the infrastructure layer directly affect the applications layer.

Business Applications Layer

Applications software components provide specific computer system solutions that meet the core business needs of SAVIN programs. Examples of applications components include:

□ Line-of-business applications supporting specific SAVIN program business needs

□ Expanded application offerings providing new capabilities to SAVIN program users

□ Defined interface requirements provided to SAVIN service providers and development staff with clear guidance for SAVIN program transactions with acquired and existing systems

□ Database management systems used to store data within the business applications

These applications support operations for SAVIN program agencies, and directly affect the infrastructure layer by creating and altering infrastructure requirements based on application requirements. The applications layer also forms the foundation upon which the publication layer distributes information.

Publication Layer

Publication components provide information to SAVIN program users from existing systems. Examples of publication components include:

□ Secure web portals providing access to existing information

□ Indices enabling complex searches and faster access

□ Global search engines providing single-point access

□ Data-transformation services delivering aggregated information to users

□ Subscription and notification systems providing mechanisms to notify users that information is available

□ Standard reports generated from the business applications

The publication layer communicates the information gathered by the applications layer to the internal and external justice agencies in a useful manner. Automated communication through subscription and notification mechanisms can form a rudimentary integration framework. However, the integration layer provides a more robust platform from which to exchange data among agencies.

Integration Layer

The integration layer expands upon the capabilities in the publication layer by moving the information from one system to another as part of a business process. Information exchanged in this manner frequently forms the basis for automated action within the business application and process. Integration components exchange information between existing systems. Examples of integration components include:

☐ Batch interfaces that move information between systems at predetermined times
☐ Real-time interfaces that move information between systems as the business system records the information
☐ XML structured documents providing flexible interfaces that contain varied data and allow common interface paths.

The integration layer also creates capabilities used by the strategic and tactical analysis layer by enabling data collection and aggregation during business processing.

Strategic and Tactical Analysis Layer

This layer represents the "top" of the pyramid and is also the most difficult to attain. It depends upon all the underlying layers to function correctly and provide the information necessary to conduct the analysis for critical decision making. Analysis components provide complex relational information to SAVIN program users from existing information systems. Examples of analysis components include:

☐ Summary data sets used to build comprehensive data warehouses for offender information
☐ Decision-support systems, which represent the most complex form of criminal justice system aggregation and utilization and generally use this warehoused data that include offender data, victim and witness information, statistical information, work flow and outcomes
☐ Analytic tools, including management and reporting capabilities that report caseload, case flow, and staff information in a presentation for the user

The business value created by using information from this layer is very high, but the cost, difficulty, and management necessary to achieve the desired results from the investment are also high.

Governance Layer

The management or governance components represent the complex tasks of managing IT investments, projects, and service delivery. As shown in the pyramid, the management layer runs throughout all other layers to ensure proper operations and coordination. While this layer does not represent a particular technology component, proper technology management ensures that the technology employed meets the business needs in a sustainable manner through planning, standards, and oversight. Examples of the management components include:

☐ Organizational structures, processes, standards, and guidelines in place to plan and select projects, as well as monitor the agencies' overall IT investment
☐ Documented and enforced project management standards and processes
☐ Trained project managers who administer the project within the technical environment based on the project management standards and processes

☐ Identification and management of inter-project dependencies

☐ Use of defined systems development standards and methods

Systems and Technology

In order for a SAVIN system to provide accurate, timely and relevant information and notification end users, two types of systems must be involved:

1. The originating system that generates the data
2. The victim information and notification system that receives the data provided, translates the data, and delivers the information via automated notification

There are many criminal justice system agencies that send data to a SAVIN system, which serves essentially as a communication mechanism to provide information and notifications to end users. Any automated victim and information system, therefore, must have the capability to receive data from multiple information management systems utilizing different types of technology, accurately translate the data received, and deliver timely notifications to a registered victim or other end user.

Information management systems and technology required to support a victim information and notification service include the following:

☐ Jail Management Systems (JMS) are used by local and county jail facilities to manage individuals who are incarcerated in their facility, and include information important to victims such as: offender name and demographics, date of incarceration, projected date of release, bail or bond information, release date, etc.

☐ Law Enforcement Records Management Systems (RMS) are used by local law enforcement agencies to record crimes and incidents and report the progress of investigations. Examples of information contained in these systems include victim and witness information, suspect or arrestee data, addresses charges and disposition information.

☐ Offender Management Systems (OMS) are typically seen in prison settings and are used for managing offenders during incarceration. Examples of the data housed in these systems that would be important to victims includes: offender name and demographics, location of offender, type of sentence, length of sentence, projected release date, parole hearing dates, hearing outcomes, dates of release, revocations, dates of re-incarceration, etc.

☐ Case Management Systems (CMS) are most often used by a prosecutor’s office, court, or probation and parole agencies, and can provide a victim information and notification system with details about events such as hearing dates and times, updates or changes in charges, or the disposition of a case.

Connectivity

Since all above systems send data to the SAVIN system simultaneously and continuously, connectivity addresses how remote facilities physically access the provider’s SAVIN hosting facility to send data. The SAVIN system must effectively integrate information from multiple systems, and therefore must be able to use various types of communication methods to connect with remote systems, while maintaining the security and integrity of the data. Whenever possible, the SAVIN system should use a State’s network infrastructure, and adhere to all cyber security requirements and identity management rules such as requirements on usernames and passwords.

A SAVIN system should allow users to locate offender information in a format that is easy to access, efficient, easily understood and convenient for them. Registered users who wish to receive automated notifications should have multiple options available for delivery and receipt of the information. Users should be able to choose one or more methods, to increase the chance of guaranteed delivery of the information critical to their safety. Information and notification methods should include the following:

□ Telephone - SAVIN systems should provide an Interactive Voice Response (IVR) capability for inbound communication. The IVR system must be able to handle multiple languages spoken by system users, either by in-house operators with translation skills or by the use of an outside vendor for translation. The system must have sufficient capacity to ensure that it will generate no busy signals or dropped call situations during an inbound call. The technological capabilities must ensure that users can search for an offender and register for notifications using only a telephone while also providing for the ability at any time for users to reach a live operator/customer service representative to assist them.

□ Outbound phone communication in the form of notification must be initiated within 15 minutes after the data are received by the victim information and notification system. Outbound systems must have the ability to initiate notifications to as many phone numbers as may be required to ensure that any and all registered users receive notification immediately. Although not required, utilizing Text to Speech (TTS) and Short Message Service (SMS) capabilities to pronounce the variable information would provide for a more effective SAVIN system and are highly recommended.

□ Web Portals -SAVIN systems should provide public access to information through a web portal. The public access portal must be able to provide access to only offender information as allowed by the laws governing the jurisdiction and in accordance with agency policy. SAVIN systems must also provide a secure administrative portal through which monitoring and managing the system can occur. Both web portals should conform to Section 508 of the Rehabilitation Act (29 U.S.C. 794d). All video content on websites should include closed-captioning for hearing impaired end users.

□ Email - SAVIN systems must provide the capability to automatically send outbound email notifications of events to registered users. Emails must be sent within 15 minutes after the data are received by the victim information and notification system.

□ Telecommunications Device for the Deaf (TTY or TDD) - SAVIN systems should provide, at a minimum, the capability for automated TTY or TDD services for registered users who are Deaf or hearing impaired. The SAVIN system must be able to provide the same information on an inbound call and outbound notifications for TTY or TDD as available through the IVR capability. The scripts for notifications to hearing impaired system users must be adapted in collaboration with representatives of the Deaf community. The TTY or TDD services must be scalable so that the system provides minimal busy signals during an inbound call attempt and provides the capability to make all outbound TTY or TDD notifications within 15 minutes of the data being received by the victim information and notification system. Other adaptations may be recommended for SAVIN systems by representatives from the Deaf and hearing impaired community in collaboration with the state SAVIN Program Managers and representatives from the SAVIN Governance Committee (SGC) and SAVIN service provider.

Information Sharing Standards

Information sharing standards reduce unnecessary (and potentially wasteful) variation in the technology portfolio by establishing and enforcing best practices. Each of these standards is a necessary component for effective governance of a SAVIN technology portfolio. The standards initiatives described below provide highly relevant applications for SAVIN systems.

□ National Information Exchange Model (NIEM)

NIEM is a foundation for information exchange. It offers a common vocabulary so that when two or more people talk to each other, they can exchange information based on common words that both understand. This standard provides a data model, governance strategy, methodologies, training and technical assistance to assist users in adopting a standards-based approach to exchanging information.

NIEM's common vocabulary of terms features an information exchange platform allowing different systems to communicate without the development of custom or "stovepipe" solutions for SAVIN purposes. NIEM exchanges exist for many of the frequently utilized justice and public safety information sharing transactions, and can be leveraged by SAVIN systems to effectively enable information sharing across internal systems, as well as with other partners and jurisdictions. Additional information on NIEM is available at www.niem.gov.

□ Global Federated Identity and Privilege Management (GFIPM)

GFIPM provides a framework for identification/authentication, privilege management, and audit to access applications. GFIPM methodology can be utilized to ensure that security and authentication policies are enforced throughout the system since it provides the definition and management of access privileges to the applications and data contained in the systems involved in the victim information and notification applications and databases. It also provides the efficiencies of a single sign-on protocol for all authorized system users, avoiding redundancy and providing cost-reduction savings. Additionally, eXtensible Access Control Markup Language (XACML) provides a standards-based infrastructure for exchanging information about the access control and privacy policies of protected resources in terms of the elements in the metadata model.

SAVIN systems can leverage Security Assertion Markup Language (SAML), which is an XML-based framework for specifying authentication information about a user. It allows for assertions to be made regarding the identity, attributes, and entitlements of each user. These assertions are passed from one business entity, Partner Company, or application to another. The audit aspect of GFIPM helps determine what information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data access and management practices.

□ Global/Justice Reference Architecture (GRA)
GRA provides a proven template solution and a common vocabulary with which to discuss implementations (often to stress commonality). It leverages the best practices of industry and, more specifically, the Organization for the Advancement of Structured Information Standards (OASIS) Reference Model for Service-Oriented Architecture (SOA). The GRA, based on long-time industry standards and best practices, links the various standards available, such as NIEM and GFIPM, and provides a consistent, uniform approach to managing technology resources to support information sharing. GRA also supports the necessary linkage between systems interacting with the victim information and notification systems. Deliverables from the GRA project can help with developing business architecture (e.g., service identification and design guidelines), information architecture (service modeling guidelines), and technology and solutions architecture (execution context guidelines and service interaction profiles) components. The GRA approach utilizes a natural and cohesive grouping of technologies, standards, or techniques in meeting service development requirements.

□ SAVIN National Standard
Work performed by industry and subject matter experts in 2011 resulted in the development and testing of a Victim Notification (VN) Service that standardizes automated information sharing for victim information and notification and serves as the SAVIN National Information Standard (SAVIN National Standard). The Victim Notification (VN) Service is National Information Exchange Model (NIEM) and Global Reference Architecture (GRA) conformant which includes data elements and definitions for the exchanges of offender information from a criminal justice "notifying agency" system (such as a County Jail or a Court) to a Victim Notification Provider (VNP) system. This SAVIN National Standard provides for timely status information updates and notification of key events to victims and interested parties. The SAVIN National Standard also provides for a standardized information exchange to be used between notifying agency systems and victim notification systems.

These information sharing standards help standardize automated information sharing among all the stakeholders involved in the victim information and notification process. With increased information sharing it is also important to ensure that proper security and privacy guidelines are in place.

Security and Privacy

Because the privacy of victim-related information or a victim's request to receive information is critical, SAVIN systems must adhere to the rules of the FBI CJIS Security Policies, and in particular, CJIS encryption requirements. Due to the variety and complexity of the security rules associated with the messages exchanged between the systems submitting the data to victim information and notification systems (and the significant differences from jurisdiction to jurisdiction), a comprehensive authorization and access control mechanism, based on GFIPM, should be put in place for the implementation of this service. In many cases, simply divulging the existence of information is equivalent to disseminating the information itself. Implementers must take care to ensure that appropriate authorization and access controls are in place even when exchanging seemingly benign information flags indicate information availability.

Laws that prohibit or otherwise limit the sharing of personal information vary considerably among jurisdictions and agencies. The Privacy Act of 1974 (5 USC §552a) as amended, other statutes such as the E-Government Act, and many government-wide or departmental regulations establish a framework and criteria for protecting information privacy. This would allow implementation of the guidelines defined by the Global Privacy Technical Framework. The memoranda of understanding (MOUs) among participating entities can further define specific privacy requirements.

Key Resources

There are many key resources available through the following website links:

- □ SAVIN Online Community: www.savinonline.org
- □ SAVIN Notification Service Specification Description Document: www.savinonline.org
- □ NIEM Website: http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1012
- □ GRA Website: http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015
- □ Global Federated Identity and Privilege Management: htts://www.it.ojp.gov/gfipm
- □ Privacy and Civil Liberties: http://it.ojp.gov/default.aspx?area=privacy
- □ FBI CJIS Security Policy: http://publicintelligence.info/CJISsecuritypolicy.pdf
- □ Section 508: http://www.section508.gov