SAVIN

STATEWIDE AUTOMATED VICTIM INFORMATION AND NOTIFICATION (SAVIN)

SAVIN TECHNOLOGY ROADMAP

Final Version	**23 December 2014**
Sponsoring Organization	**Bureau of Justice Assistance** Office of Justice Programs U.S. Department of Justice
Authoring Organizations	**IJIS Institute** www.ijis.org **National Criminal Justice Association (NCJA)** www.ncja.org

This project was supported by Grant No. *2010-VN-CX-K080* awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This work is a collaborative effort of the National Criminal Justice Association and the IJIS Institute, under the sponsorship of the Bureau of Justice Assistance of the Office of Justice Programs at the U.S. Department of Justice. The support and participation of BJA in the project is greatly appreciated.

The specific contributions of the SAVIN Technology Roadmap Focus Group provided insight into the technology issues and challenges related to the provision of victim notification services and were critical to the generation of the *SAVIN Technology Roadmap*. Creating this document to be a functional description of SAVIN technology needs would not have been possible without the direct input from these practitioners, stakeholders, technology experts, and others engaged in the field provision of victim services:

Jamie Freestone, SAVIN Program Coordinator
Division of Criminal Investigation, South Dakota Office of the Attorney General

Michael Overton, Chief, Information Services Division
Nebraska Crime Commission

Joan Eliel, Investigator/Program Specialist
Montana Department of Justice

John Daugherty, Chief Information Officer
Montana Department of Corrections

Travis A. Fritsch, Domestic Violence Specialist
Domestic Violence Consulting Services (Lexington, Kentucky)

Heidi Smith, SAVIN Program Manager
North Dakota Criminal Justice Information Systems

Daniel M. Foro, Senior Advisor
New York State Sheriffs' Institute

Brent Meyers, Director, Registration and Victim Services
Central Office Agency, Indiana Department of Correction

Bureau of Justice Assistance (Project Sponsors)

David Lewis, Senior Policy Advisor, Justice Information Sharing

Todd Maxwell (Booz | Allen | Hamilton)

SAVIN Project Staff

Ashwini Jarral, Director
IJIS Institute

Bob May, Assistant Director
IJIS Institute

Kathy Gattin, Senior Project Manager
IJIS Institute

Trudy Gregorie, National SAVIN TTA Project Team, Senior Director
Justice Solutions

Anne Seymour, National SAVIN TTA Project Team
National Crime Victim Advocate

Tammy Woodhams, National SAVIN TTA Project Team, Senior Staff Associate
National Criminal Justice Association

IJIS Institute Member Companies

Paul Wormeli, Owner/Consultant
Wormeli Consulting, LLC

Jim Pingel, Integration Practice Manager
URL Integration, Inc.

Bob Slaski, President
Open Networks, Inc.

Don Dinulos, Sr. Consultant, MCSD, MCAD, MCTS (BizTalk)
Microsoft Enterprise Services, Justice and Public Safety

Todd Tincher, Director, Professional Services
Appriss

Specific recommendations in the *SAVIN Technology Roadmap* regarding information safeguarding were contributed by Todd Tincher from Appriss.

Most importantly, the rationale for even discussing this issue is to serve the victims of crime that are traditionally not well represented by the criminal justice system in its normal process of adjudication and supervision. It is the strong hope of the authors and participants in this effort that these recommendations regarding a technology roadmap will serve to improve and extend services to the most important stakeholders—the victims of crime.

1. INTRODUCTION

Technology has always been an essential element of Statewide Automated Victim Information and Notification (SAVIN) programs. From the early inception of the program, technology has been the basis for allowing states to create ways for victims to register their interests in particular offenders, for data about events pertaining to these offenders to be extracted from various criminal justice information systems, and for the composition and delivery of notices to victims about relevant events. It could be demonstrably argued that without the relevant technology, it would be impossible for states to create such programs.

In the time since SAVIN programs were first initiated, several revolutions of technology have taken place, and states today have additional options and extensions of existing technology that may be considered. It is the purpose of this document to describe the technologies that are needed to implement a SAVIN program and to propose some additional tools that states may consider as they seek to enhance SAVIN services, reduce the costs associated with providing SAVIN services, or both. This document will articulate a roadmap for technology implementation in SAVIN programs by combining information on the state-of-the-art of relevant technology with the experiences and understanding of SAVIN program administrators as to what functions and baseline components should be considered and addressed by technology.

This document is intended to serve as a supplement to the SAVIN Guidelines document that was developed based on the experiences of early adopters and refined through consensus of SAVIN program administrators. These guidelines remain the primary definition of services that a SAVIN program should consider implementing, and, therefore, can be used as a potential baseline for measuring the completeness and utility of the service being provided.

In addition to aggregating the vision and program experiences of SAVIN program administrators, this roadmap will take into account and directly address some of the pertinent findings of prior assessments and notable evaluations of the SAVIN program. Of particular relevance is the evaluation project conducted by ICF International under the auspices of the National Institute of Justice.[1]

Previously drafted SAVIN technology guidelines that have been endorsed by a set of SAVIN program administrators have been replicated in this roadmap to ensure consistency with the guidelines and provide a common framework for the technology recommendations developed.

By addressing both prior evaluations and current technology trends, the roadmap presented here is aimed at providing guidance to SAVIN program administrators. It is also meant to comprise a set of best practices with respect to the applications of technology in SAVIN to support the deliberations of funding authorities and others interested in program outcomes. It is informative to take into account past evaluations of statewide victim information and notification services. In the most recent evaluation conducted under the auspices of the National Institute of Justice, "service providers reported that the most common challenges experienced by both themselves and their clients were inaccurate notifications and/or delayed or outdated notifications. A couple of service providers reported hearing of instances where

[1] Evaluation of the Statewide Automated Victim Information and Notification Program, Final Report, October 2013, https://www.ncjrs.gov/pdffiles1/nij/grants/243839.pdf.

inaccurate, delayed, or absent notifications allowed offenders to show up at victims' homes and, in some cases, re-assault them."[2]

The concept of a roadmap, as used in this report, defines the functional requirements that technology must support, concentrating on the business processes that should be at the heart of designing a solution for victim notification. The roadmap does not attempt to provide detailed designs for applicable technology, leaving that work to the implementing organization. The *SAVIN Technology Roadmap* is also meant to be vendor agnostic and as universally applicable as possible; whether systems are internally constructed or outsourced, the business processes to be supported remain the same.

The logical endpoint of the development of a technology roadmap for any specific SAVIN program will lead to the development of a procurement instrument. Regardless of whether the intention is to build such a system with internal state resources or hire a company to build and implement the system, it is strongly recommended that a request for proposals (RFP) be written to make as clear as possible the functionality expected of the building organization. Such an RFP should remain as a functional statement of the characteristics that the system should exhibit, without attempting to describe needless detail on how to construct the system.

Appendix C presents an example of an RFP that stems from a technology roadmap and is functional in nature. While this example does not attempt to cover all of the components discussed in this report, it illustrates the kind of document that will be useful in implementing any SAVIN technology roadmap.

1.1. METHODOLOGY

The *SAVIN Technology Roadmap* was created by a focus group of SAVIN program administrators and other knowledgeable participants including states that are relatively new to the program as well as those having had implementations for some time.

Both large and small states were included in the focus group. The focus group's discussions and input formed the basis for NCJA and IJIS Institute staff to expand on the principles and content addressed by the focus group and to conduct further research to define the roadmap. The focus group included an audience of experienced administrators, victim advocates, technology experts, and others to gain a consensus from the participants who have a stake in the operation and outcomes of SAVIN programs. Comments and contributions from the focus group members, the larger reviewing audience, and staff were incorporated in the final *SAVIN Technology Roadmap*.

[2] Evaluation of the Statewide Automated Victim Information and Notification Program, Final Report, October 2013, https://www.ncjrs.gov/pdffiles1/nij/grants/243839.pdf.

2. TECHNOLOGY PLANNING – THE PRECURSOR

Planning for the implementation of technology to support a SAVIN program or to examine the potential for enhancement of existing programs is certainly a critical part of the technology roadmap, and is as important as in any other major system. It has been well established that a strategic plan or vision, and the establishment of a governance process, are key starting points for any multi-jurisdictional system and SAVIN is no exception. Concepts and recommendations about governance and the development of strategic plans are provided in the basic *SAVIN Guidelines and Standards*[3] and supported in other literature. The *SAVIN Technology Roadmap* Focus Group addressed some of the key governance issues as they relate to technology.

The technology planning process begins with developing a clear understanding of the mission and purpose of a system. It includes gaining a thorough understanding of the requirements and constraints embodied in existing programs, statues, and executive policies that will place boundaries as well as define the authorized scope of a victim notification system. From this point, the task of the SAVIN management team is to clearly define a scope of work for the system, including an architectural prototype that answers questions about the kind of system that will be operated and identifies the stakeholders and processes that will be the foundation of the system.

In support of the planning process, one of the most useful approaches is to document the workflow that the system will follow, and to note the points of intersection with other systems and the points of notification that will be made, or the event in the process where a notification will take place. Documenting the workflow and the requirements for each process, and the output of processes as they are linked together, will help define the technology requirements for the support of a SAVIN program.

At an early point in the planning process, either for initial implementation or for considering upgrades or expansions to service, it is very helpful to consider the approaches taken by other states in implementing specific functions and to understand lessons learned in doing so. An ongoing collaboration among SAVIN program administrators can be a useful tool in helping individual states understand the opportunities for, and challenges of, advancing victim notification services across state boundaries.

As a part of the strategic planning process, either initially or in an update to the plan, it will be important to define the high-level technology requirements needed to operate the program. Many states have found the process of issuing a Request for Information (RFI) to prospective technology providers helpful in defining the possibilities and the technology.

The desired end result of the above suggestions should be a strategic plan that incorporates the intent of acquiring technology needed to support all of the components of the victim notification services to be offered. A good strategic plan will begin with the business processes and, from these processes, derive the technology requirements and articulate the kinds of technology that will be incorporated in the system.

It should be noted that in these times of rapid technological obsolescence, the strategic plan is not simply a one-time document that languishes while the technology revolution that occurs every three years or more frequently bypasses the organization. Strategic plans, more specifically their technology

[3] http://it.ojp.gov/documents/ijis_savin_guidelines_standards.pdf

components, should be updated at least every two years, and plans laid for the acquisition of technology that will improve services or reduce costs for the program.

Finally, it has been noted by numerous observers and practitioners that the SAVIN program should not be considered as a standalone, stove-piped system. It is, or should be, a component of a broader criminal justice information sharing environment where the concept of notifying both victims and criminal justice practitioners is an extension of the requirements that should be at the basis of any criminal justice information sharing system. More specifically, at the very point where an event related to an offender is initially scheduled or occurs, the trigger to notify any victims that have registered their interest in a particular offender should automatically initiate the notification process. As legacy systems are replaced by more modern, component-based systems, this principle should be a normal part of the design process so that the extraction of event data and construction of the victim notification repository is an essential element of the specifications for a new system. Grant-making authorities should encourage agencies to make such a requirement of any new system being developed that entails tracking of events relative to offenders.

Support for the notion of a holistic view of the justice information sharing environment is an essential part of the President's *National Strategy for Information Sharing and Safeguarding* that is now the fundamental platform for creating information sharing environments. Helpful goals and objectives in the *National Strategy for Information Sharing and Safeguarding* support the concept of a wholly integrated criminal justice information system implementation and provide a clear path for state and local decision makers to view a way forward for national information sharing.[4]

[4] See the National Strategy for Information Sharing and Safeguarding at: http://ise.gov/sites/default/files/2012infosharingstrategy.pdf.

3. SAVIN TECHNOLOGY COMPONENTS

Technology is at the heart of victim notification services. It is safe to say that victim notification programs would be very difficult to implement without technology. However, there are always specific requirements to be met and boundaries or constraints to be applied in the acquisition of technology.

For the purposes of describing the technology that is the basis of current and future victim notification systems, we can organize the discussion around the basic business processes that are essential in a victim notification program: registration, offender data collection and repository building, and notification processes.

3.1. Registration Process

Victim registration has been most frequently implemented using a call center where victims can call and register their interest in a particular offender by speaking with a call center operator. The basic technology in the call center approach is a telephone system that can handle and route calls to a variety of answering points.

The registration function in a SAVIN system is designed to provide a way to register an interest in a specific offender and to provide contact information and choice of the means for notification. While the primary purpose of registration is to allow victims to register their interest, some states have determined that the capability should also be made available to law enforcement and justice personnel who may also register their interest in tracking the events related to a specific offender. The registration function allows the victim or professional to indicate which offender is of interest, to express a choice of the events that are of interest for notification, the contact information for the victim or professional, and the preferred and alternative means of notification. The objective of the registration process is to build a database that stores the offenders of interest, the persons interested in them, the events that are of interest, and the contact information and preferences for notification of the victims or professionals having submitted their interest.

To accomplish this task, most SAVIN programs 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 through the use of third-party or external provider for language translation services. 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 for users to reach a live operator/customer service representative to assist them at any time during the call.

SAVIN programs should include a Telecommunications Device for the Deaf (TTY or TDD) interface so that SAVIN can 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 also be able to provide outbound notifications to hearing impaired message recipients via TTY/TDD; the hearing impaired community must be provided with the information a non-hearing impaired person could search for through an automated IVR type of service. The SAVIN program should also have the capability for delivering these messages and notifications via automated services.

The scripts for notifications to hearing impaired system users must be adapted in collaboration with representatives of the hearing impaired community. The TTY/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/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.

As the technology of web services has progressed in recent years, many SAVIN systems have implemented, or are considering using, web portal technology to provide the capability for victim registration or public access to information. While there are other options, SAVIN systems can effectively use a secure administrative portal through which monitoring and management of the system can occur. The primary purpose of the portal is to allow victims to register interest in a particular offender. The public access portal must be able to provide access to offender information only as allowed by the laws of the authority having jurisdiction and in accordance with agency policy. Depending on whether the state has chosen to operate an open or closed system, there may be multiple variations of the portal to serve the general public, victims, and criminal justice agencies. With the explosion of mobile device usage, and the statistics that show ever-increasing access to websites via mobile devices, it is incumbent on SAVIN systems to incorporate a mobile version of the portal that can be used on the various mobile device operating system environments. Another factor to consider is that any and all versions of a SAVIN web portal should conform to Section 508 of the Rehabilitation Act (29 U.S.C. 794d).[5]

3.2. Offender Data Collection and Notification

The SAVIN program defines a set of events related to the status of the offender, which become the subject of a notification to the victim. There are two functional capabilities that the technology must support in order to complete this process. First, the creation or designation of a central data source or system(s) for the events upon which a notification will be made with links to the corresponding offender(s). Second, the submitting system must be able provide and send data regarding the event to initiate the victim notification process when the event occurs.

The objectives of the data collection process are to:

1. Provide the information from various submitting systems pertaining to an event of interest to the victim or other registrant

2. Translate such event information into what will become a notification.

3. Link event data with the offender information – containing the victim/interested person information collected as a part of the registration process – and initiating triggers that will activate the notification process.

SAVIN programs recognize that the acquisition of event data to be part of a notification comes from external systems that are primarily serving the law enforcement or justice agencies having the responsibility to schedule and carry out such events. For example, scheduling trial dates is under the

[5] http://www.section508.gov/Section-508-Of-The-Rehabilitation-Act

authority of the courts, various hearings are under the auspices of multiple adjudication agencies, parole hearings under the authority of the parole board, etc. The SAVIN program bears the responsibility of identifying the potential sources of data and working with the agencies owning the process by which the data are collected so that there can be an extraction of data used to populate the SAVIN central repository.

Data describing events defined as status changes are the foundation of victim notification, and can potentially come from a variety of city, county, regional, and state information management systems. Technology required to support a victim information and notification service includes the capability to extract data on the occurrence of selected events from the following categories of systems:

- **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.

Most SAVIN programs have reached out initially to traditional criminal justice institutions as sources of information (e.g., courts, probation, prisons, jails and supervision authorities). While many offender-related events are tracked and managed by these institutions, the increasing use of diversion as an alternative to incarceration brings new challenges to SAVIN programs; these programs are now exploring the addition of status and event reporting from diversionary programs, adding the event of being assigned to such a program and the release or transfer out of such a program to the list of proscribed events that are tracked by SAVIN and subject to the issuance of notifications. Victims are particularly interested when such programs include partial or temporary work or other release events. Temporary releases should be supported by the system.

The contribution of community service agencies and specialty courts, such as drug courts, is an important part of providing full victim notification services, and the SAVIN technology should support obtaining offender tracking information from all such agencies.

While many of the events being tracked, which are triggers for notification, are fairly simple statements (nature of the event or change in status, the anticipated date, and the reference information on participation in the event that must be displayed in the notification), there are some events that require special handling. For example, in many states, victims are entitled to have a recent photograph of the offender at the time of release from corrections. The SAVIN technology must accommodate updates to photographs from correctional or possibly other agencies and be able to acquire and post such images. It is generally recommended that when photographs of the offender are upgraded prior to release that victims be able to opt-in to or opt-out of receiving such updates.

Network connectivity is also a key function that must be provided in order to collect the data. Since all of the systems previously described 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, including requirements for user authentication and authorization.

Victims, as well as criminal justice professionals, depend on the notification services from SAVIN for very important information that may affect their safety or that of the public. Therefore, one of the functions that is essential in SAVIN systems and requires technology to accomplish is the continual monitoring of the linkages that provide the data collection and processing function. SAVIN systems generally seek to create a *heartbeat* function that tests the connectivity frequently to ensure that the link remains in a working condition and that events are indeed being reported to the central repository as planned and promised.

3.2.1. The Role of Standards in Data Acquisition

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. While not an exhaustive list, the standards initiatives described below provide highly-relevant applications for SAVIN systems.

National Information Exchange Model (NIEM)—NIEM is a foundation for information exchange that provides a common vocabulary of terms allowing different systems to communicate without the development of custom or stovepipe solutions for SAVIN purposes. NIEM exchanges exist for many of the frequently used 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.

Federated Identity and Privilege Management—Federated identity and privilege management solutions such as the Global Justice Information Sharing Initiative (Global) Federated Identity and Privilege Management (GFIPM) program provides a framework for identification/authentication, privilege management, and audit to access applications. GFIPM methodology can be used 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 the potential for cost 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, 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)—The Global/Justice Reference Architecture (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 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 uses a natural and cohesive grouping of technologies, standards, or techniques in meeting service development requirements.

SAVIN program administrators would be wise to remain aware of trends and advancements in information sharing and safeguarding as there are developments that are continuing to occur that may help improve efficiency in SAVIN systems and even help lower costs. For example, web services continue to be built into standards for information exchanges by the Global Advisory Committee to the Attorney General under the Global Standards Council. As these message standards are adopted for information sharing purposes, they can be used in the provision of SAVIN services as well.[1]

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.[6] The VN Service is a NIEM- and GRA-conformant national information standard (including 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. The SAVIN National Standard provides for timely status information updates and notification of key events to victims and interested parties. The 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.

3.2.2. Linking Offender Information for Victim Notification

SAVIN programs are faced with the challenge of aggregating information collected from the various contributors of event information. The preferred method is to base the combination of data on a state identification number, system or offender identification number, Federal Bureau of Investigation (FBI)

[6] http://it.ojp.gov/gist/131/Victim-Notification--VN--Service-Specification--Version-1-0

number, or other fixed number associated with the individual offender, particularly when based on fingerprint or other biometric identification. However, in all cases there may not be such a number to use. The absence of such a number does not relieve the state of the responsibility to make the connection. The following provides an example of how one state, North Dakota, has addressed the linkage problem:[7]

> North Dakota (ND) SAVIN received federal funds to implement Registration Link, which is a service that allows victim registrations to seamlessly transition when an offender transfers to a new facility, to parole/probation, or back into a facility from parole/probation. Originally, we had anticipated linking to court notifications, as well; however, this was removed from scope due to technical limitations.
>
> **Product Features**
>
> Specifically, ND Registration link provides ND SAVIN with the following features:
>
> - Allows offenders that are transferred to different facilities or to/from parole/probation to be linked. This then allows registrations to be transferred so that victims will be notified as the offender moves through facilities in ND.
> - Provides a mechanism to automatically match records in the ND VINE system, based on matching rule sets, to allow victim registrations to seamlessly transition with the offender record.
> - Provides county transfer notification generated to let the registrant know that their registration(s) could be transferred within the next 72 hours and that if we are not able to transfer their registration(s), they will be notified again and provided instructions on how to re-register. If the offender is not matched, a notification will be triggered to let the registrant know they have to re-register because their registration(s) could not be transferred.
> - Provides reporting on the results of the matching process. Registration LINK will be able to generate a pending notification record to queue a notification to the victim letting them know whether or not their registration has been linked to a new record.
>
> **Product Description**
>
> The ND SAVIN system has been configured to identify offenders across registrations and match them to each other based on the availability of data from the North Dakota systems that were determined during implementation.
>
> An OML (Offender Mapping Logic) client was developed that contains a set of offender mapping logic. The following criteria has been developed for linking logic to begin:
>
> - Offender to Offender – Criteria – Transfer Status

[7] Provided by Heidi Smith, SAVIN Program Director, North Dakota.

- Offender to Probationer/Parolee – Criteria – Transfer Status
- Probationer/Parolee to Offender

The following data elements will be available for defining matching rules:

- First Name, Last Name, Alternative ID(s), Agency, DOB, Gender, SSN, Race

The OML below is what was configured for North Dakota.

- Offender to Offender – Criteria – Transfer Status.
    - Agency must use a transfer record for the matching logic to link.
    - North Dakota has a statewide ID that is being used by the DOCR and Probation Department. Matching is already taking place without the use of a transfer record, since a statewide ID allows that to be processed. These matches are taking place outside the Registration Link Service and were not part of the Registration Link reporting.
    - Linking does not occur if the matching offender record is set to be purged from the system, if the offender is blocked for registrations or the agency is disabled for registrations.
- Offender to Probationer – Criteria – Transfer
    - Agency must use a transfer record for the matching logic to look for a link.
    - Linking will occur if the offender record is in a transferred status. The probationer record can have any supervision status.
    - Linking will not occur if the probationer record is set to be purged from the system or if the probationer is blocked for registrations or if the agency is disabled for registrations.
- Probationer to Offender
    - Probationers/Parolees in the Probation Module will automatically link when the offender appears in the county jail.
    - Probationer/Parolee to DOCR is already in place due to the statewide ID being used by both agencies. These matches were taking place outside of the Registration Link Service and are not be part of the Registration Link reporting.

3.2.3. Safeguarding SAVIN Information

SAVIN program administrators bear a direct responsibility for safeguarding SAVIN information, particularly with respect to personally identifiable information (PII) regarding victims of crime. One of the ways that SAVIN programs will be judged by the community to be effective is in the extent to which they inspire confidence around the protection of data collected.

One way to instill that confidence is through excellent security practices. Good security practices can be broken into four main areas:

1. Protecting data from misuse by authorized individuals.
2. Having and following a process for granting access to new users.
3. Protecting the databases and messages.
4. Understanding and enforcing permissible use of data.

3.2.3.1. Protecting Data from Misuse by Authorized Individuals

As stewards of data, it is important to have in place technology for monitoring system transactions along with a process to alert a supervisor or some other individual in authority when misuse of the system is detected. Misuse could be, but is not limited to, the following:

- Accessing data for personal use, e.g., looking at information about one's neighbor.
- Selling or distributing data for personal gain, such as to a bail bond agency.

Using technology audit trails can be automatically scanned and algorithms can be developed to report abuse. The audit trails will track the queries by person and the algorithm would track the normal usage of that individual and flag them when they run more queries than normal. A report would be created by the system and sent to the administrator for review. This approach eliminates the need to check all queries and only focus on those outside the norm.

3.2.3.2. Process for Granting Access to New Users

Lack of control in how new users are added and granted access to their data is another area of concern for data contributors. Using GFIPM as part of the SAVIN program, along with a single sign-on, can provide the authentication and authorization controls that assure the creation of a trusted link between users and the system.

3.2.3.3. Protecting the Databases and Messages

Data contributors want to know that safeguards are in place to protect against unauthorized access and intruders. Given that the SAVIN system is, or should be, part of an effective criminal justice information sharing environment, the need to adhere to FBI standards for systems that may be connected to its central Criminal Justice Information Systems (CJIS) databases is paramount. The principles of safeguarding that are contained in the FBI CJIS rules are also sound and sufficient for ensuring safeguarding of data in systems such as SAVIN, and the incorporation of technology to support the FBI standards is highly recommended.[8]

3.2.3.4. Understanding Permissible Use

Each contributing agency also requires that the data they contribute is being shared with the appropriate personnel. A robust implementation of the GFIPM standard, including both the authentication protocols and the privilege management functions, will handle this requirement.

3.3. Notification Services

Having created the capability for victims and criminal justice professionals to register their interest in events regarding specific offenders, and having created a collection system to determine when such events will occur or have occurred, the final process of SAVIN services is to make a notification to the registrant. The basic functions in this process are to initiate the contact with the registrant, deliver the message regarding the event, and to confirm that the message was received.

The SAVIN system should be able to meet the needs of victims as well as criminal justice professionals. In both cases, registrants should be able to express interest in events applicable to a specific offender and to be notified when such events occur or are scheduled. There are certain events where automatic notification should be enabled by the supporting technology. For example, offender releases or escapes should result in a notice to relevant law enforcement agencies.

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. Basic SAVIN systems employ the following alternative information and notification methods:

- **Telephone** – SAVIN systems typically provide an IVR capability for notification. 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.

- **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.

With the substantial penetration of smartphones and other mobile devices, states are considering expanding notification services using social networking applications. It is feasible to make notifications to personal and direct messaging features in Twitter, Facebook, and other social media systems. Making this form of notification an option for victims would require changing the registration system to allow for these new messaging options, and giving victims the capability to select these media. The difficulty of using these media to confirm receipt of such a message makes the choice of social media more of a back-up, secondary notice than a primary notification option. However, future versions of the mobile

[8] FBI Security regulations can be found at http://publicintelligence.info/CJISsecuritypolicy.pdf.

applications may well support the kind of Application Programming Interfaces (APIs) that would complete the feedback loop. For supporting mobile interfaces to SAVIN systems, it may be particularly useful to enable Text to Speech (TTS) and Short Message Service (SMS) capabilities to actually speak the message in order to provide for a more effective SAVIN system.

Another possibility is the creation of a mobile application for victim notification. Such an app could be used for registration, general inquiry on offender status, and for notification of events when connected to an Internet session. The disadvantage of such an approach is the reliance on Internet connectivity to enable the two-way link required for acknowledgement of the notice.

3.3.1. Measuring SAVIN System Performance

A highly-desirable function to be included in SAVIN applications under all classes of media used for notification is the measurement of customer satisfaction and performance of the SAVIN system. States will inevitably derive their individual metrics for measuring performance, but the technology built for the operation of the system is the logical vehicle for gathering the data on system performance and customer satisfaction. Notifications could include in the acknowledgement function an indicator of customer satisfaction and such responses could then be analyzed and reported to program sponsors.

The performance management function can be executed through technology that would allow independent feedback from victims and other users, as well as supporting periodic surveys of customer satisfaction.

3.3.2. Interstate Exchange of Notifications

While a detailed design is yet to be worked out, the interstate exchange of victim notification services remains an important objective of the SAVIN program. As victims move or offenders are relocated, the SAVIN systems must provide a way to make modifications of the notification components to sustain the notification service. When offenders are relocated to other states, the sustainment of victim notification services means that the victim registration would have to be transferred from one state to another. Similarly, when offenders are relocated, the connections to new fundamental sources of event information would have to be linked to the victim registration system.

The Interstate Commission for Adult Offender Supervision has developed an Interstate Compact Offender Tracking System (ICOTS) that was designed to track the location of adult offenders and has implemented the agreements between states for exchanging the data on offender relocation.[9] The commission is in the process of working out how victim notification systems should interact with the ICOTS transfer of information, and a coordinated and integrated exchange of victim information, as well as offender information, is the goal of current deliberations.

However the design comes to fruition, participating states are likely to agree on using the SAVIN specification as a basis for exchanging information, and, therefore, the SAVIN technology should anticipate the use of this standard. The capability to generate a message based on the SAVIN standard should be an essential component of the SAVIN software.

[9] http://www.interstatecompact.org/ICOTS/WhatisICOTS.aspx

One of the important functions that the technology must support is maintaining the rights, privileges, and control of the data. As information is passed from state to state, there is an issue of defining the steward of the data and allowing updates and edits to the data. An important component of the agreement between states for handling the transfer of victim information is the definition of rights and privileges for data modification or deletion.

4. SYSTEMS ADMINISTATION AND RELIABILITY

There are three main components of SAVIN system reliability.

1. Availability,
2. Integrity of the system, and
3. Protection against a catastrophic event.

4.1. Availability

SAVIN systems receive and provide data on events that can occur at any time and can impact public safety; as such, it must be available 24-hours-a-day, 365-days-a-year. The system must have minimal disruptions, and a very short weekly maintenance window that occurs at a regular, posted day and time that is least impactful on the system operation. (Maintenance messages should be available on the phone and website for public information during the outage window.) The SAVIN system should conform to the same availability metrics and service levels defined for other mission-critical systems such as Computer Aided Dispatch (CAD) and law enforcement and criminal history records systems. Statistics that record the SAVIN system's availability must measure components at the hardware and software level and be documented and monitored by the SAVIN program manager. Statistics related to availability should be regularly reviewed by designated personnel within the lead agency, the SAVIN Governance Committee, and SAVIN service provider.

4.2. Integrity of the System

The SAVIN program must provide capabilities to ensure that the ongoing integrity of the system is intact. The system must provide the capability to:

- Detect, by location, and notify the SAVIN administrator when data is not being sent to the system.
- Detect and notify when the system is unable to receive data.
- Detect and notify when erroneous data is being sent (or suspected of being sent) to the system.
- Detect and stop unauthorized use of the system.
- Detect and stop attempts to hack into the system.
- Detect and synchronize duplicate data being provided from multiple systems.

4.3. Protection against a Catastrophic Event

This planning would cover a single system component outage to multiple system component failures or loss of a complete facility. To protect against this type of outage, the SAVIN system must provide the following:

- Backup procedures in the event of any failure. The offline storage media from the scheduled system backups (programs and databases) must be stored in a protected, off-site location that can be quickly returned and recovered in case of a failure.

- A warm central backup site available for the system so that services can be restored in a matter of hours in case of a catastrophic failure. A warm site is defined as a separate environment having the computing environment and software available and with data replicated on the warm backup site so that no (or minimal) restores are required, if needed.

5. CONCLUSIONS

Each and every state will have its own technology roadmap for implementing and enhancing SAVIN. This report is merely a guide to creating such a plan, and makes no claim to be universal. The one truth we do know is that no such technology roadmap is static. The need for challenging the status quo is ever present, and the opportunities for change are frequent and constant. Annual reviews and projections should be the norm for any SAVIN system.

As in any IT system in criminal justice, the technology roadmap for SAVIN is impacted by the rapid pace of technological change and also by expanding and varying policy changes about the services to be provided. For a system that serves the public, it is incumbent on the administrating agency to:

- Remain aware of and to incorporate new technologies that will improve service, particularly when they also may reduce costs, and

- Reflect changes in policy, whether by statute or administrative procedure, as soon as possible after adoption.

The needs of victims should always drive the continuous improvement of SAVIN systems, by making this service easier to use and more complete.

Making SAVIN a more integral part of the criminal justice information sharing objectives as a part of a true information sharing environment will help make the SAVIN service more complete, and exploring the contemporary technologies of social media, mobile devices, and advanced software for information sharing will reveal opportunities to improve the delivery service. SAVIN system administrators can never relinquish their attention to the importance of monitoring event sources and delivery systems to ensure that the notifications are delivered as promised if these systems are going to stand.

Intrastate and interstate victim notification systems will be most efficient and accurate when the SAVIN specification is fully adopted in all SAVIN systems for the data collection and for the intersection between systems affecting SAVIN operations.

Finally, there can be no rest for all involved in the support of victims until the stakeholders implement victim notification on a national scale, making it possible to exchange data on both offender and victim relocations without requiring reregistration.

6. APPENDICES

The following appendices contain supporting information and additional resources.

6.1. Appendix A: Acronyms and Abbreviations

ACRONYM OR ABBREVIATION	DEFINITION
API	Application Programming Interface
BJA	Bureau of Justice Assistance
CAD	Computer Aided Dispatch
CJIS	Criminal Justice Information System
CMS	Case Management System
DOJ	U.S. Department of Justice
FBI	Federal Bureau of Investigation
GFIPM	Global Federated Identity and Privilege Management
Global	Global Justice Information Sharing Initiative [DOJ]
GRA	Global Reference Architecture
ICOTS	Interstate Compact Offender Tracking System
IVR	Interactive Voice Response
JMS	Jail Management System
ND	North Dakota
NIEM	National Information Exchange Model
OJP	Office of Justice Programs
OMS	Offender Management System
PII	Personally Identifiable Information
RFI	Request For Information
RFP	Request for Proposals
RMS	Records Management System
SAML	Security Assertion Markup Language
SAVIN	Statewide Automated Victim Information and Notification
SGC	SAVIN Governance Committee
SMS	Short Message Service
SOA	Service-Oriented Architecture
TDD/TTY	Telecommunications Device for the Deaf
TTS	Text-to-speech
VN	Victim Notification
VNP	Victim Notification Provider
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

6.2. Appendix B: Key Resources

For further information on many of the topics in this roadmap, there are many key resources available through the following website links:

- SAVIN Online Community: www.savinonline.org
- SAVIN Notification Service Specification Description Document: http://it.ojp.gov/gist/131/Victim-Notification--VN--Service-Specification--Version-1-0
- NIEM website: www.niem.gov
- GRA website: https://it.ojp.gov/GRA
- Global Federated Identity and Privilege Management: http://www.gfipm.net
- Privacy and Civil Liberties: http://it.ojp.gov/default.aspx?area=privacy
- FBI CJIS Security Policy: http://publicintelligence.info/CJISsecuritypolicy.pdf

6.3. Appendix C: Example RFP Statement of Work

The following is an excerpt from the Montana Department of Corrections Request for Proposal illustrating the specifications requested for the implementation of SAVIN in Montana. This excerpt was provided by John Daugherty, Chief Information Officer, Montana Department of Corrections, and is reprinted with permission.

The successful bidder must:

1. Demonstrate its experience and capability in the implementation and customization of a victim-centered automated information and notification system that was used successfully in another state department of corrections in a production environment. The system must have met all guidelines and standards established by the U.S. Bureau of Justice Assistance (BJA) for Statewide Automated Victim Information and Notification (SAVIN) programs.

2. Provide a user-friendly automated toll-free telephone registration process available (24) hours a day, seven (7) days a week that allows registrants the choice to self-register for notification using a touchtone telephone following voice-recorded prompts, or register “live” using a rotary, touchtone or cell telephone with the assistance of a call center operator. This automated information and notification system will provide accurate and timely messages to registrants when a change occurs in the custody status of an adult offender under MDOC supervision. Callers will be able to obtain the current custody status of an offender under MDOC supervision with or without registering for future notifications. Available information will include the offender’s current custody status (prison, prison alternative, probation or parole), the location of the offender (facility location or city in which the offender is supervised on probation or parole), scheduled release dates, and the month of any scheduled parole hearings. Registrants may choose

to register for email, text messaging, or telephone notification, or any combination they choose. All notifications will be sent by CONTRACTOR to registrants in the manner chosen by the registrant.

3. Establish and maintain a call center twenty-four (24) hours a day, seven (7) days a week, staffed by operators who are employed by the Contractor. Operators must be trained to (a) hear concerns of victims in crisis and respond immediately in a manner that conveys trust and competence; (b) report the current custody status of any adult offender under MDOC supervision, (c) upon request from the caller, provide referrals to Montana crisis centers and other community victim services, and (d) assist callers in the use of the victim information and notification system. The call center must be accessible with a toll-free number to anyone within the United States and be capable of TTY method of notification/communication for the hearing impaired.

4. Provide a user-friendly public website available (24) hours a day, seven (7) days a week that allows registrants to access the current custody status of any adult offender under MDOC supervision, self-register for notification, and view a tab containing Montana-specific victim services information. Contractor will promptly update the information upon request of MDOC staff. Registrants may choose to register for email, text messaging, or telephone notification or any combination they choose.

5. Transfer and update offender information from the Offender Management System or OMS to the Contractor with updates to take place at intervals mutually agreed upon by the Contractor and MDOC, including near real time.

6. Notify registrants (24) hour a day, seven (7) days a week when an emergency custody status change occurs. Emergencies include offender escape or a facility crisis that could pose an immediate safety risk to victims and/or the public, such as a fire, inmate uprising/riot, act of war or terrorism, or natural disaster. Emergency notifications must begin within fifteen (15) minutes of when the Contractor's call center receives the emergency information from MDOC. Emergency notifications must continue every 30 minutes or until the registrants have been notified.

7. Provide an override feature that allows MDOC staff to trigger an immediate emergency notification.

8. Provide a global notification procedure whereby all registrants can be notified about unusual situations that affect their safety or security.

9. Provide an "exception" process whereby Contractor can delay notifications if an unusually high number of outgoing notifications queue up.

10. Notify registrants about non-emergency custody offender status changes between 7 a.m. and 9 p.m. seven (7) days a week. Call patterns will be mutually agreed upon by Contractor and MDOC staff.

11. Provide a Personal Identification Number (PIN) mechanism, or equivalent, for registrants to confirm and stop calls once they have received notifications.

12. Provide samples of notification scripting that invites victims' trust and demonstrates that the Contractor understands victims' unique needs for safety and security, confidentiality, and accurate, timely offender information.

13. Ensure incoming calls to the call center are not placed on hold or in a caller queue for an extended period of time. MDOC defines an extended period of time as anything longer than 15 seconds.

14. Establish and maintain a secure administrative web portal that allows select MDOC staff to enroll registrants for notification. This site will also provide statistics and audit reports on all notification calls that the system processes. Every message is logged to provide assurance of the system's performance.

15. Demonstrate the experience, ability, and willingness to work with MDOC's victim program manager and Information Technology (IT) staff to (a) learn about MDOC facilities, offender population, and Montana's unique victim notification needs, and (b) promptly resolve problems ranging from interpersonal communications to technical issues.

16. Provide strategies for educating the public and training MDOC staff and other Montana victim service providers in the use of the notification system.

17. Schedule onsite training with MDOC up to twice a year during system rollout and up to once a year in subsequent years, and ongoing web-based training for MDOC and non-MDOC program managers and volunteers who collaborate with MDOC to provide education and services to crime victims in Montana.

18. Provide MDOC-specific printed and electronic public education and training materials annually as follows: up to 4,000 brochures and 100 posters that describe how to access and register for the notification system; up to 50 training DVDs for MDOC and county victim/witness advocates, and 100 pens with the MDOC system logo for promotional purposes.

19. Communicate via telephone conference call with the MDOC victim programs manager and Information Technology (IT) staff on a mutually acceptable schedule up to twice monthly.

20. Immediately report all concerns, breakdowns, and other issues to designated MDOC contacts.

21. Following contract execution, successful bidder must provide MDOC with project details including data file layouts, milestones, and scripting of inbound and outbound messages.

System and Technical Requirements

1. The notification system must be able to accept offender movement and correctional status changes from MDOC at regular intervals throughout the day, seven (7) days a week.

2. At a minimum, Contractor must provide a secure FTP site to receive correctional status events from MDOC that will initiate a notification. MDOC's preferred method of interfacing is web services. The Contractor will use web services to exchange the correctional status events utilizing XML conformant to the NIEM XML schema for this exchange. The web service must

conform to SOAP standard for implementing web services and use W3C XML Schema validation to verify the data payload conforms to the NIEM standard. A document explaining the standards is available upon request.

Contractor Requirements

The successful bidder (Contractor) must:

1. Agree that offender data provided to the vendor for the purpose of notification to registrants remains the property of MDOC and will not be used for any other purposes without the written permission of the MDOC.

2. Agree that information provided by registrants for notification purposes remains the property of MDOC and will not be used for any purpose. The vendor must make available to registrants, at the time of registration, a privacy statement that details the use of their information.

3. Demonstrate the ability to achieve at least a 99.95 percent redundant process, as required by BJA standards, to avoid any downtime due to hardware, software, or power outage issues.

4. Demonstrate the ability to provide uninterrupted service in the event of a long-term power outage, natural disaster, or hardware failure at Contractor facilities.

5. Demonstrate characteristics of a notification system implemented on established, proven technology platforms that most users will readily accept, including user-friendly screens and navigation, sound data navigation rules and error messages that maintain system quality.

6. Provide security features that will

   a. prevent unauthorized individuals from accessing any information pertaining to registrants, or state information

   b. ensure that data transmission, processing, and storage are secure; and have the capability to back up records stored electronically and prevent unauthorized access to, or amendment of, these records.

Deliverables

Bidders must submit with their bid response a detailed list and timetable for deliverables needed to be achieved by the State and the successful bidder in order to meet the timelines established. This information must be mutually agreed upon between the State and successful bidder.

Demonstration

The state reserves the right to request a demonstration of the notification system offered by the [apparent] low bidder in order to verify compliance with the bid specifications. This demonstration may be performed via web-based meeting or may be performed on-site – as determined by the bidder. The demonstration will be provided by the bidder within 5 business days of the request – unless otherwise agreed to by the state and the bidder.