DRAFT

Bureau of Justice Assistance
U.S. Department of Justice

Global Reference Architecture

Statewide Automated Victim Information and Notification (SAVIN)

Victim Notification (VN) Service Service Description Document

Version 1.0.0

December 2012

Global Justice Information Sharing Initiative

Global Information Sharing Standard

Global Standards

The collection of Global-recommended normative standards has been developed and assembled into a unified package of composable, interoperable solutions that enable effective information exchange. This collection is known as the Global Standards Package (GSP). GSP solutions are generally focused on resolving technical interoperability challenges but also include associated guidelines and operating documents to assist implementers. The GSP includes artifacts associated with many of the Global product areas, including but not limited to:

- **Global Reference Architecture (GRA):** Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- **Global Service Specification Packages (SSPs):** Reference services that are reusable nationwide in order to save time and money and reduce complexity when implementing particular information exchanges with external partners.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing security, identity management, and access control solutions to ensure that information can be accessed only securely and appropriately.
- **Global Privacy Technology Framework:** A framework for automating information access controls based on privacy and related policies restricting the use or dissemination of such information.

For More Information

For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit http://www.it.ojp.gov/gsc.

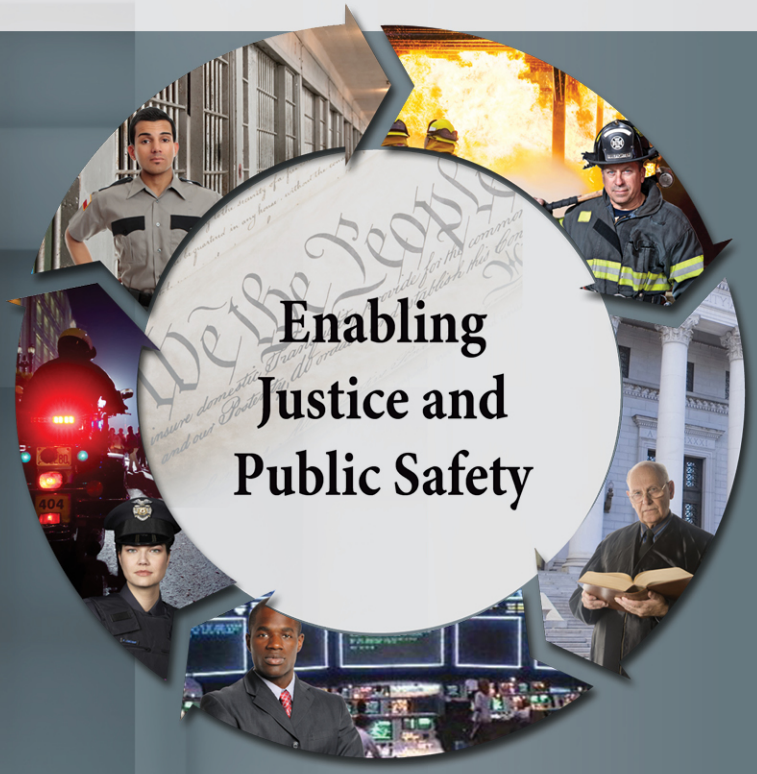

Table of Contents

1. Document Introduction

This document is designed as a Service Description for the Victim Notification (VN) Service.

In the context of the Global Reference Architecture (GRA) and Service-Oriented Architecture [SOA] in general, a service is the means by which one partner gains access to one or more capabilities offered by another partner. Capabilities generate real-world effects that can be as simple as sharing information or can involve performing a function as part of a complex process or changing the state of other related processes. Government organizations have numerous capabilities and a multitude of partner organizations, both inside and outside of their traditional communities. There are significant benefits to these organizations for sharing information and having access to each other's capabilities. Achieving interoperability among these organizations requires alignment of business and technical requirements and capabilities. In addition, it is critical to have a consistent way of specifying these requirements and capabilities and sharing them across organizational boundaries. The GRA was developed to facilitate interoperability and to assist in meeting other key requirements common in a complex government information sharing environment. In order to achieve interoperability, a consistent approach must be defined to identify, describe, and package services and their interactions in many different technical environments, across multiple government lines of business, at all levels of government, and with partner organizations.

The GRA defines a service interface as "the means for interacting with a service." It includes specific protocols, commands, and information exchange by which actions are initiated on the service. A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the "how" of the interaction. Since the service interface is the physical manifestation of the service, best practices call for service interfaces that can be described in an open-standard, machine-referenceable format (that is, a format that could automatically be processed by a computer).

A Service Specification is a formal document describing the capabilities made available through the service; the service model that defines the semantics of the service by representing its behavioral model, information model, and interactions; the policies that constrain the use of the service; and the service interfaces that provide a means of interacting with the service. A Service Specification is analogous to the software documentation of an Application Programming Interface [API]. It provides stakeholders with an understanding of the structure of the service and the rules applicable to its implementation. It gives service consumers the information necessary for consuming a particular service and service providers the information necessary for implementing the service in a consistent and interoperable way.

The main components of a Service Specification are the Service Description, one or more Service Interface Descriptions, and the schemas and samples used to implement and test the service.

A Service Description contains information about all aspects of the service that are not directly tied to the physical implementation of the service; in other words, the service interface. A Service Interface Description is a description of the physical implementation; specifically, the service interface used in a specific implementation of the service.

2. Service Overview

2.1 Purpose

The Victim Notification (VN) Service is designed as a standard for providing timely information and notification of key events to victims.

2.2 Scope

The VN Service is a National Information Exchange Model (NIEM)- and Global Reference Architecture (GRA)-conformant national information standard for the exchanges of offender information and notifications from a criminal justice "notifying agency" system to a Victim Notification Provider (VNP) system.

Victim registration and access to the VNP, as well as the actual notification delivery to the victim, are the responsibility of the VNP and are not in the scope of this service.

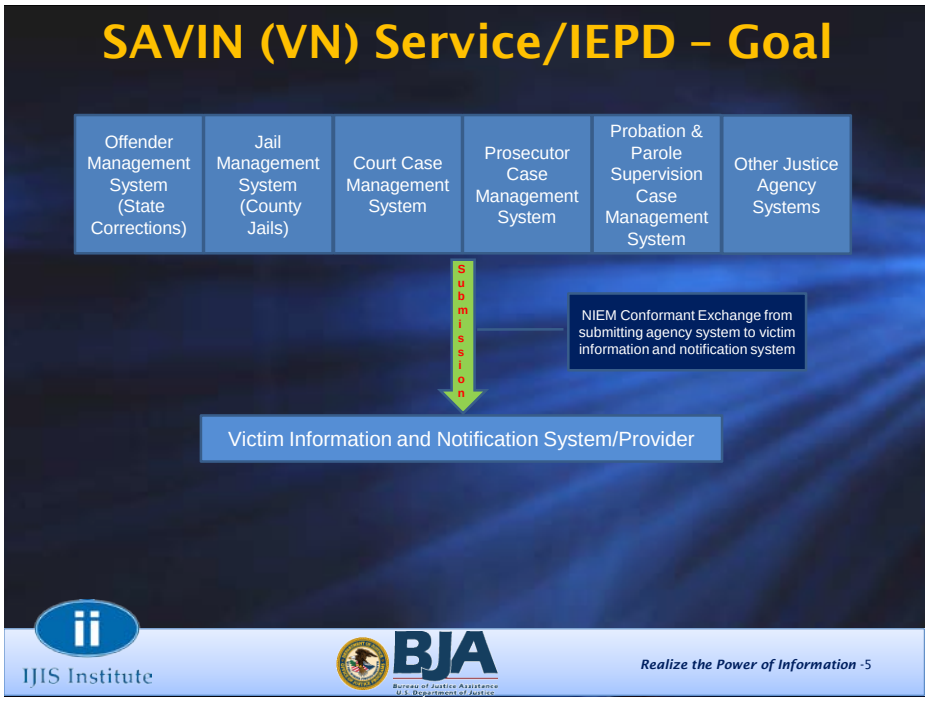

Figure 1: SAVIN (VN) Service Goal

2.3 Capabilities

1. Offender Information (e.g., new offender, updated offender data) is possessed by notifying agencies.[1] This service provides these agencies with the capability to exchange offender information with a victim notification provider (VNP).

2. Notification information is produced when a triggering event occurs in an agency.[1] This service provides notifying agencies with the capability to exchange event notification information with a victim notification provider (VNP).

2.4 Real-World Effects

At a high level, the VN service provides offender information to a VNP. It also provides VNPs with event notification information collected from multiple criminal justice agencies as an offender traverses the criminal justice system. Crime victims have a right to receive notification when offenders have specific types of interactions within the criminal justice system. The VN service provides a standardized information exchange to be used by notifying agencies that are responsible for providing offender and event notification information, which may reside in various systems, and sharing that information with VNPs.

[1] Refers to agencies required to participate in the victim notification process by law, as well as those agencies willing to participate.

Agencies,[1] and victim information and notification programs that operate at a state or jurisdictional level, benefit from this capability in a number of different ways. For example:

2.4.1 Notifying Agency

Statutory requirements to notify victims of specific events in the criminal justice process (and the data related to these events) are an important step in keeping victims informed. Occasionally, errors occur and victims are not notified. Notifying agencies that are responsible for providing offender and notification information can use this service to ensure that the information is delivered to a VNP.

The notification of victims can take many forms (mail, phone, e-mail, etc.). Many agencies are required to submit notification information to victims of crime, but the method of notification can add complexity to the process. For example, the prosecutor's office could become aware of a hearing about which the victim needs to be notified. The prosecutor's office updates its records and sends a request to victim services to notify the victim. Victim services then sends an e-mail to the victim with the court date. The prosecutor in this example, the notifying agency that is responsible for providing notification information, can use this service to automate the process so that the information is delivered electronically to a VNP when an entry is made in the case management system (either the court's or the prosecutor's computer system).

2.4.2 VNPs

One of the primary tasks of a victim information and notification program is to receive, collect, and provide notification information in the form of a notification message and deliver these notifications to the victim. The VNP does not control or determine the timeliness of the notification message but is responsible for the processing and delivery of a notification to the victim(s). VNPs using this service can reduce the notification lag time (event to notice) significantly, since the service allows for real-time exchanges.

Event notifications can vary a great deal across jurisdictions regarding content, timeliness, etc. Untimely, incorrect, and hard-to-understand notifications confuse victims. This service utilizes a standardized data exchange. For example, the definition of "hearing" can vary across agencies. The service glossary defines "hearing" so that any system using the service can convey accurate information. In addition, the service should incorporate business process rules which will help alleviate confusion. For example, duplicate notifications, multiple notifications for the same event, and notifications showing an offender in two places at the same time are not allowed.

2.5 Summary

Notifying agencies will use this service to send VNPs information about an offender and victim notification events.

2.6 Description

The Victim Notification (VN) Service facilitates cross-jurisdictional data sharing to inform Victim Notification Providers (VNPs) about an offender's interaction with the criminal justice system. This service can facilitate the ability to share offender information and provide event notification information. Specific interactions with an offender result in information being sent to a VNP. The details will include information about the agency involved, relevant dates, identifiers (e.g., case number, ID number), and the disposition or status of the event.

2.7 Security Classification

The highest level of security classification for the information exchanged by this service is Sensitive But Unclassified (SBU). As a result, the service can be assigned a security classification of SBU.

2.8 Service Specification Package Version

This service specification is built based on version 1.0.0 of the Service Specification Package.

3. Business Scenarios

The Victim Notification (VN) Service focuses on the exchange of information between notifying (criminal justice) agencies that are responsible for providing offender and event notification information and VNPs. Notifying agencies that are responsible for providing offender and notification information will use this service to provide VNPs:

1. Offender Information

2. Event Notification Information (an event that requires victim notification)

3.1 Primary Flow

- A Notifying Agency system (which provides offender and notification information) generates an event notification message.
- The Notifying Agency system sends the message to the VNP system.
- The VNP system receives the message.
- The VNP system processes the message.
- The VNP system generates an event notification response message.
- The VNP system sends the event notification response message to the Notifying Agency system.
- The Notifying Agency system receives the response message.
- The Notifying Agency system processes the response message.

The following diagram depicts the process flow described above:

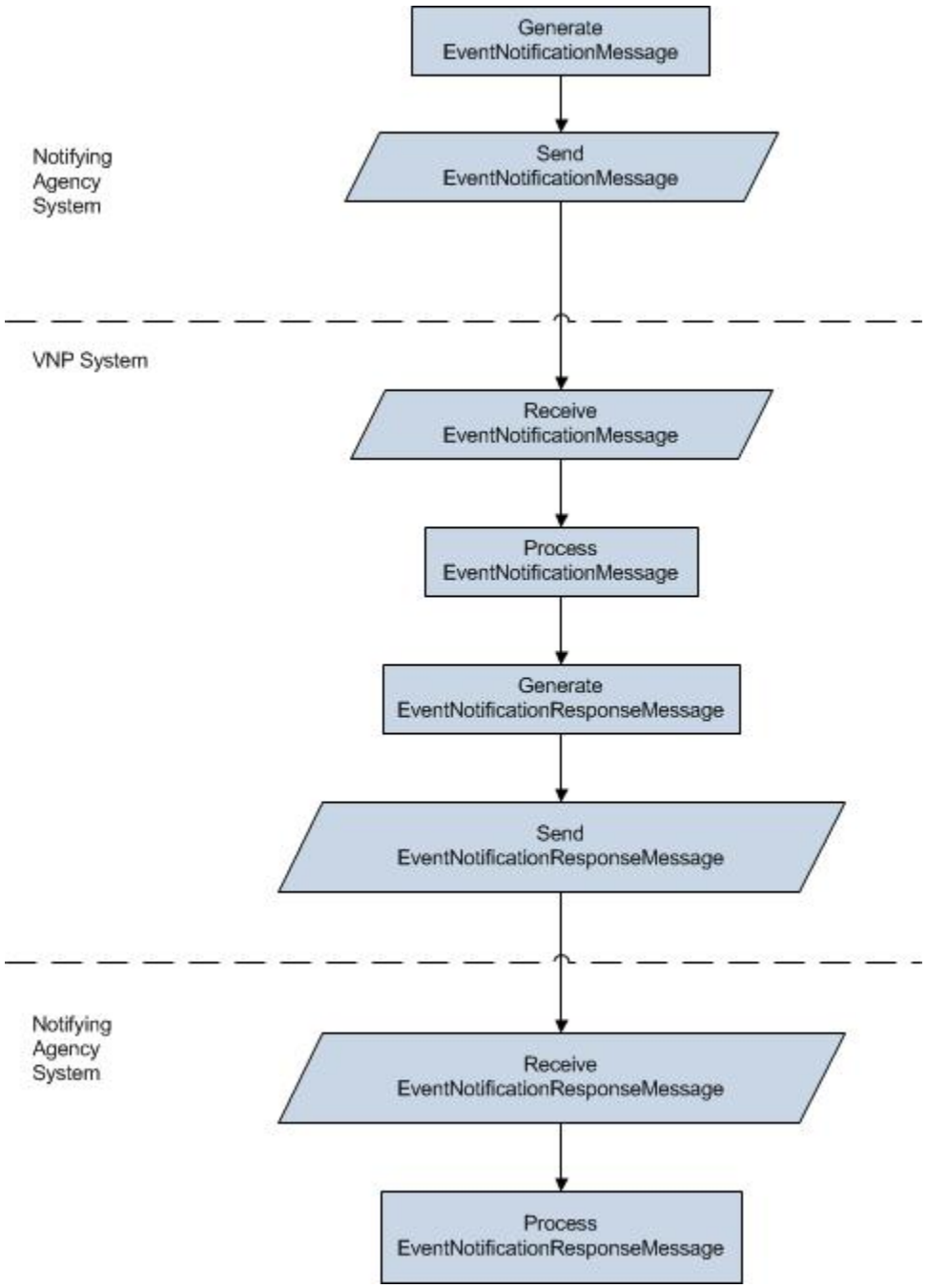

Figure 2: VN Process Flow Diagram

4. Service Interoperability Requirements

4.1 Service Assumptions

- Key information relating to messages exchanged is stored in a log file for

auditing purposes. An audit service should be used to perform the audit function, since this is an important process of the overall victim notification business process.

- All messages exchanged will require a synchronous acknowledgement of receipt.

- The acknowledgement of receipt will contain only metadata about the message. The metadata will consist of a time stamp and identifiers that uniquely identify the message.

- Messages other than the synchronous acknowledgement or fault (e.g., VN response message) are returned asynchronously. Consequently, requesting systems must implement a service endpoint to receive these responses.

- The service implementation has no means to identify responding systems. That is, the service specification does not specify how the service might locate responding systems of interest. In practice, the identities of responding systems may be hardcoded in the service implementation, or the service may use an electronic directory to locate provider systems.

4.2 Service Dependencies

No dependencies have been identified at this time.

4.3 Execution Context

The service design will follow the GRA Execution Context Requirements.

4.4 Policies and Contracts

Participating entities will use memoranda of understanding (MOUs), non-disclosure agreements (NDAs), service-level agreements (SLAs), or other types of agency agreements as appropriate to document applicable policy requirements.[2]

4.5 Security

- The service implementation must adhere to the rules of the CJIS Security

[2] See Global policy documents at http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015.

Policies, in particular, CJIS encryption requirements.

- Because of the variety and complexity of the security rules associated with the messages exchanged by the VN Service and the significant differences from jurisdiction to jurisdiction, it is recommended that a comprehensive authorization and access control mechanism based on GFIPM is in place for the implementation of this service.

4.6 Privacy

- The MOUs between participating entities will further define specific privacy requirements.

- Because of the variety and complexity of the privacy rules associated with the messages exchanged by the VN service and the significant differences from jurisdiction to jurisdiction, it is recommended that a comprehensive authorization and access control mechanism based on GFIPM be in place for the implementation of this service. This would allow implementation of the guidelines defined by the Global Technical Privacy Framework.

Note that, 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 flags that indicate information availability.

4.7 Additional Information

4.7.1 Timeout and Exception Handling

The functionality of the service includes an asynchronous response. Implementers are responsible for determining appropriate timeout periods, cases of response messages received after a timeout has expired, and appropriate handling of response messages that indicate some sort of problem.

4.7.2 Intermediary

The implementation of this service should include an intermediary system (e.g., broker), as discussed in the Global Execution Context Guidelines.

5. Service Model

5.1 Information Model

5.2 IEPD Reference

The VN Service uses the VN IEPD for all messages exchanged by the service. The IEPD is included in its entirety in the artifacts/service_model/information_model folder of the Service Specification Package.

5.2.1 Data Inputs

Event Notification Message

A Notification Message is used by a notifying agency that is responsible for providing offender and notification information to the VNP. The submit message contains information about the offender (e.g., biographical data), sending agency (e.g., incident/case number, agents), and details pertinent to the event.

Event Notification Response Message

An Event Notification Response Message is used to provide the notifying agency with any details that the VNP needs to return—which, at a minimum, consists of the receipt of the submit message. The response message returns one of two values—information pertinent to the agency that provided the offender notification information, or an error in processing the request (i.e., because of a system problem).

5.2.2 Data Outputs

All actions of the service return a synchronous acknowledgement or fault message. The acknowledgement message indicates that the input message was successfully received and provides identifiers that can be used to correlate an asynchronous response to the original input message. The fault message indicates that the input message could not be processed, including the reason for the failure.

5.2.3 Data Provenance

The data exchange by this service originates at the notifying agency that is responsible for providing offender and event notification information. The provenance of the data will be restricted to the data provided by the specific sending partner agency.

5.3 Behavior Model

5.3.1 Action Model

Included in this section are the actions defined by the VN service.

Action Name	EventNotification
Action Purpose	
This action will be implemented by the VNP to receive an Event Notification Message.	
Action Inputs	Action Outputs
EventNotificationMessage	Acknowledgement or Fault
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

Action Name	EventNotificationResponse
Action Purpose	
This action will be implemented by the Notifying Agency to receive an Event Notification Response Message.	
Action Inputs	Action Outputs
EventNotificationResponseMessage	Acknowledgement or Fault
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

5.3.2 Process Model

The information flow diagram, sequence diagram, and business process modeling notation (BPMN) diagrams provided below further describe the behavior model of the service. These diagrams are also included in the artifacts/service model/behavior model folder of the Service Specification Package for reference.

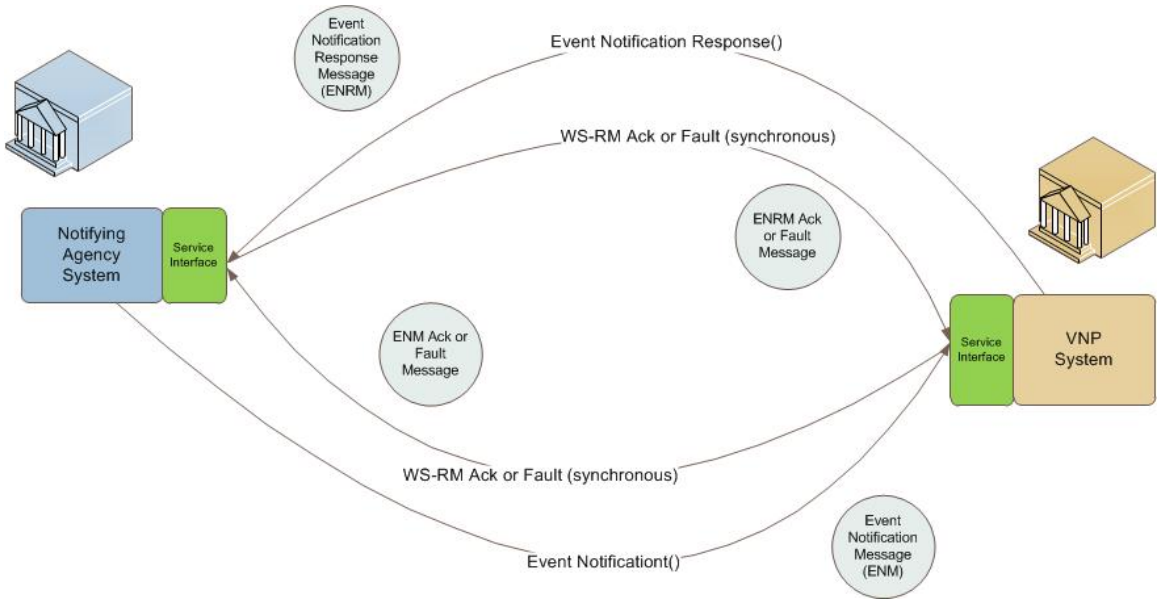

Figure 3: VN Information Exchange Flow Diagram

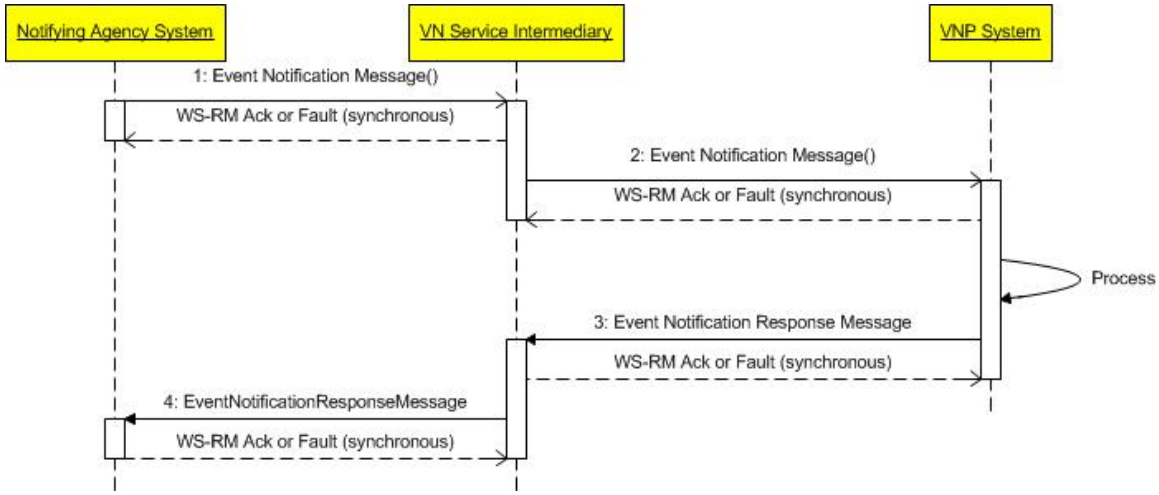

Figure 4: VN Sequence Diagram

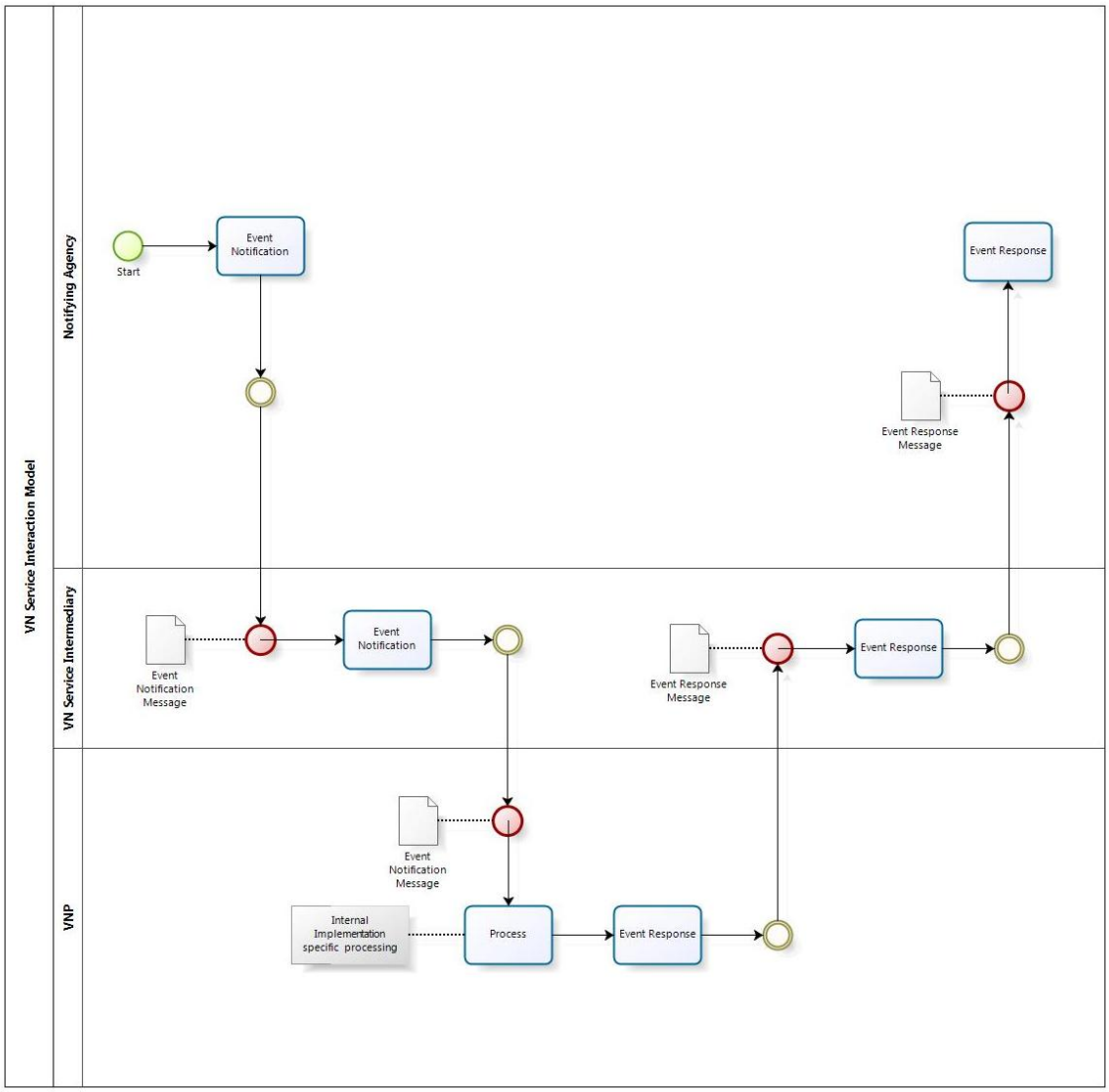

Figure 5: VN Service Interaction—BPMN Diagram

Appendix A—References

Global Reference Architecture Web Site	http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015
CJIS Security Policy	The CJIS Security Policy is considered to be Sensitive But Unclassified (SBU) material. This policy may not be posted to a public Web site, and discretion must be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice. A copy may be obtained by contacting the state's CJIS Systems Officer (CSO).

Appendix B—Glossary

VNP	Victim Notification Provider

Appendix C—Document History

Date	Version	Editor	Change
06/10/2011	0_1_0	Brad Kobishop	Initial version.
07/26/2011	0_1_1	Brad Kobishop	Updates from group review.
09/29/2011	0_1_6	Brad Kobishop	Updates from IJIS.
12/11/2011	1.0.0	Brad Kobishop	Final review.
06/18/2012	1.0.0	Global Standards Council (GSC) Services Task Team (STT)	Public comment period.
10/18/2012	1.0.0	GSC STT	Service changes received from IJIS—changes incorporated.
12/6/2012	1.0.0	GSC	Approved.

About the Global Advisory Committee

www.it.ojp.gov/global

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

For more information on Global and its products, including those referenced in this document, call (850) 385-0600 or visit http://www.it.ojp.gov/GIST.

About the Global Standards Council

www.it.ojp.gov/gsc

The Global Standards Council (GSC) serves as a Global Advisory Committee (GAC) subcommittee, supporting broadscale electronic sharing of pertinent justice- and public safety-related information by recommending to BJA (through the GAC) associated information sharing standards and guidelines. To foster community participation and reuse, the GSC reviews proposed information sharing standards submitted by Global consumers and stakeholders. Additionally, BJA emphasizes an open, participatory review-and-comment process for proposed standards; please see the Global Justice Tools Web site at www.globaljusticetools.net for more information on this opportunity. BJA-approved standards are developed, maintained, and sustained as one cohesive Global Standards Package (GSP) located at http://www.it.ojp.gov/gsp.

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.