THE DEPARTMENT OF JUSTICE'S VICTIM NOTIFICATION SYSTEM

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 08-04
January 2008

REDACTED FOR PUBLIC RELEASE

THE DEPARTMENT OF JUSTICE'S VICTIM NOTIFICATION SYSTEM*

EXECUTIVE SUMMARY

The Department of Justice (DOJ) Victim Notification System (VNS) is an automated system used by federal personnel to notify federal crime victims regarding developments in their cases, including information about the status of the investigation, prosecution, trial, incarceration, location, and custody status of the offender related to the crime.

The VNS came online in October 2001 and as of October 5, 2007, contained information on more than 1.5 million registered victims. The annual budget for the VNS has remained at approximately $5 million since fiscal year (FY) 2002.[1] Since work began on creating the system in FY 1998, the VNS has cost a total of more than $38 million. The VNS is managed by the Executive Office for United States Attorneys (EOUSA) and is used by all United States Attorneys Offices (USAO), the DOJ Criminal Division, the Federal Bureau of Investigation (FBI), the Federal Bureau of Prisons (BOP), and the United States Postal Inspection Service (USPIS).

In this audit, the Office of the Inspector General (OIG) examined the management of the VNS, the effectiveness of the VNS for victims, and the information security of the system. In conducting this audit, we interviewed personnel who managed the system, as well as personnel from agencies directly involved with the VNS. We analyzed victim-related data in the VNS and sent surveys to a sample of victims in the VNS. We also worked with a contractor to perform a review of the VNS's information security. In general, our audit covered the period from FY 1998 through FY 2007.

Results in Brief

Our audit found that, overall, federal VNS users and victims we surveyed were generally satisfied with VNS services.[2] However, we

---

* The full version of this report includes information that EOUSA considered to be sensitive, and therefore could not be publicly released. To create this public version of the report, the OIG redacted (deleted) two appendices that were considered sensitive by EOUSA, and we indicated where those redactions were made.

[1] Detailed information about VNS funding can be found in Appendix III.

[2] Federal VNS users, such as FBI Victim Specialists and USAO Victim/Witness Advocates, generally specialize in dealing with victims and victim issues and access the VNS to manage information that relates to cases in the control of their agency.

identified weaknesses in certain areas. Specifically, we found that there are few internal controls in place to ensure the accuracy and completeness of data in the VNS. For example, 18 percent of the surveys we mailed to victims considered to be active in the VNS were returned as undeliverable.[3] Officials from VNS-participating agencies also discussed with us similar problems they have encountered with undeliverable correspondence.

We also determined that EOUSA has no schedule or written plans for: (1) increasing storage space on the VNS server, despite capacity having reached a level where system performance has been affected; (2) replacing VNS hardware, which is reaching the end of its usefulness; or (3) providing for the continuity of VNS project management, which is currently concentrated in a single position.

We also found that EOUSA is now in the process of expanding the number of agencies that participate in the VNS, although it had not previously placed a priority on such expansion. In addition, EOUSA is working on establishing a direct connection for the VNS to obtain court-event data from the Administrative Office of the U.S. Courts (AOUSC). When developed, this interface will assist USAOs with notification of court proceedings.

As a result of victims' responses to our surveys indicating that they considered the custody status of defendants to be of high importance, EOUSA is now working to include such information, available from the United States Marshals Service (USMS), in the VNS.

Our review of VNS effectiveness revealed that many victim-respondents to our survey: (1) found VNS notifications to be generally understandable and useful, (2) obtained the information they desired from the VNS Call Center, and (3) found the VNS website generally easy to use.[4] However, 25 percent of active VNS victims who responded to our survey reported having no knowledge of the VNS or that their names were maintained in such a system. The fact that a significant number of federal crime victims were unaware of the system was of concern to us. Another concern we identified is that the contractor that maintains the VNS Call Center was not ensuring that a Spanish-speaking operator was on duty during all hours of operation, as required by the contract.

---

[3] Victims who are considered to be "active" in the VNS are those victims whose information is in the VNS and who are receiving VNS notifications.

[4] The VNS Call Center consists of an automated, toll-free telephone response system, as well as operators who can provide case information to victims.

We also found that a large percentage of victims had been removed from an active status in the VNS with no reason having been recorded for doing so. Removing a victim from "active" status means that he or she no longer receives notifications about case-related events. That VNS does not require a participating agency to note a reason for "deactivating" a victim, or establish any other internal control, renders this critical step more difficult to correct if in error.

In addition to the management and effectiveness of the system, we also evaluated the information security of the VNS. Using a private auditing firm, we identified deficiencies with EOUSA's implementation of systems and communications protection controls, identification and authentication, website privacy, security measures, and web application controls. These deficiencies indicate that the sensitive information contained within the VNS was not adequately protected against loss of confidentiality and the integrity and availability of data was not appropriately ensured.

Our report contains detailed information on the full results of our review of the VNS. In this report, we made 19 recommendations to help EOUSA carry out its responsibilities in managing the system.

The remaining sections of this Executive Summary describe in more detail the background of the VNS and our audit findings.

Background

The Victim and Witness Protection Act of 1982, the Victims of Crime Act of 1984, the Crime Control Act of 1990, the Violent Crime Control and Law Enforcement Act of 1994, the Justice for All Act of 2004, and the Attorney General's (AG) Guidelines for Victim and Witness Assistance established various procedures to address the needs of victims of crime.[5] Each of these contain a directive to ensure that victims are notified of significant stages and procedural developments in the criminal justice process. Notification means keeping victims aware of the status of an investigation of a crime, as well as the subsequent prosecution, trial, incarceration, location, and custody status of the offender related to the crime.

Prompted by a memorandum issued by the Office of the Attorney General, in July 2000 EOUSA entered into a contract with AT&T to create the

[5] Detailed information regarding this legislation can be found in Appendix II.

VNS and establish and staff a Call Center to assist federal and victim users of the VNS. Utilizing funds provided by DOJ's Office for Victims of Crime (OVC), EOUSA managed the development of the system. Field deployment of the VNS and Call Center operations began in October 2001, and the VNS was fully operational by January 2002.

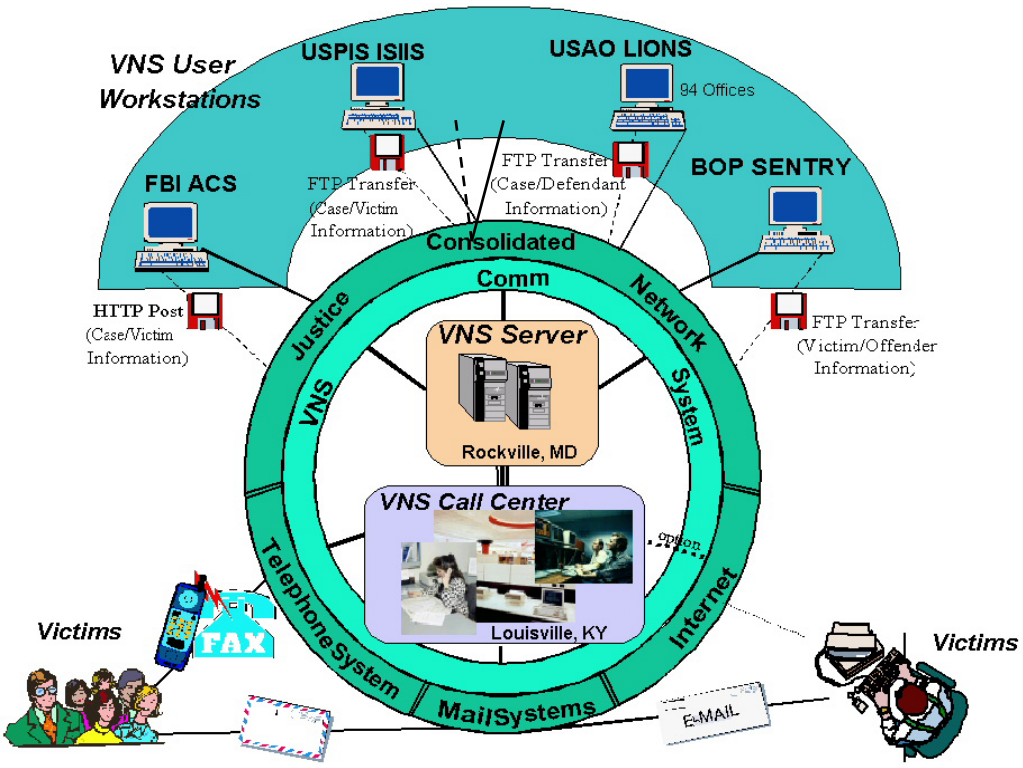
How the VNS Works

The VNS, a web-based application, receives data from automated case management systems at the FBI, USAOs, the DOJ Criminal Division, the USPIS, and the BOP. Specifically, the VNS receives downloads from the FBI's Automated Case Support (ACS) system, the USPIS's Inspection Service Integrated Information System (ISIIS), the USAO's Legal Information Office Network System (LIONS), the DOJ Criminal Division's Automated Case Tracking System II (ACTS II), and BOP's SENTRY system. Data transferred from the various systems includes the case number; victim, defendant, and inmate information; court events; and custody status updates. Notably, some of the victim-related information that resides in the VNS is personally identifiable information (PII), such as the names, addresses, and, in some cases, social security numbers of victims of federal crimes.

Victims in the VNS are notified of case events by letter, e-mail, facsimile, or telephone when a particular event in a case occurs, such as a scheduled court date or the release of a prisoner. Initially, the system consisted of the VNS, which federal VNS users access via a secure intranet connection, and the Call Center, which is used by both federal VNS users and victims of federal crimes. However, VNS services were enhanced in FY 2005 based on a DOJ request to enhance the VNS by enabling victims to access case information via the Internet. This resulted in the development of the Victim Internet System (VIS), which allows victims to have access to a subset of VNS data via the Internet. The VIS database server, in which the users' encrypted information is stored, is located at the Justice Data Center.

The following graphic illustrates how the various component systems feed into the VNS, as well as how victim users of the system obtain case-related information.

INFORMATION FLOW IN THE VNS



Source: VNS User Manual and the DOJ Criminal Division

Audit Approach

The Office of the Inspector General (OIG) assessed EOUSA's management of the VNS, the effectiveness of the VNS for victims, and the information security of the system. The objectives of the audit were to determine if: (1) EOUSA has effectively managed the VNS, including overseeing the contractors, ensuring the accuracy of data in the system, and planning for the future; (2) the VNS is an effective tool for victims of crime; and (3) the VNS was properly secured to prevent unauthorized use, access, and data modification.

To accomplish our audit objectives, we conducted more than 40 interviews with personnel from agencies directly involved with the VNS. To help evaluate the VNS's effectiveness for victims, as well as the accuracy of data in the system, we obtained and analyzed victim-related data extracted from the VNS. We then designed, deployed, and analyzed the results from surveys we sent to 2,762 victims whose status in the system was "active," as well as 480 additional surveys sent to victims who were no longer "active" in the system. In addition, we obtained a test VNS victim-user account and performed our own evaluation of various VNS services.

We also spoke with headquarters officials from those federal agencies that do not directly participate in the VNS to determine their knowledge of the system and whether they have been contacted about direct participation in the VNS. We conducted fieldwork in Chicago and Lisle, Illinois; Lexington and Louisville, Kentucky; Kansas City and Leavenworth, Kansas; and Kansas City, Missouri, where we spoke with senior management and staff who utilized the VNS at the local USAO, BOP, USPIS, and FBI offices. We also performed a limited review of the contracted services that are provided and, in order to evaluate the VNS's information security, utilized a private auditing firm to perform an information security review of the VNS.

In general, the scope of our audit covered the period from FY 1998 through FY 2007. Additional information about our audit scope and methodology is contained in Appendix I.

EOUSA Management of the VNS

Our audit determined that personnel from VNS-participating federal agencies, such as FBI Victim Specialists, were generally satisfied with services provided by the VNS. However, weaknesses remain in how calls to the VNS Call Center are tracked, the accuracy of data in the VNS, and the long-term plans for the future of the system.

Data Accuracy

We found that there are few internal controls in place to ensure the accuracy and completeness of data in the VNS. According to the VNS Project Manager, the accuracy of information in the VNS is largely dependent upon what was provided or entered originally by the participating agency, and there is no process for routinely checking the accuracy of victim files in the VNS. Yet, this means that victims whose contact information in the VNS is incorrect could be missing the opportunity to attend court events and be otherwise updated on the status of their case. EOUSA told us that it is the victim's responsibility to update all contact information. Victims can update their information by various methods, such as via the VNS website or by contacting the USAO Victim-Witness Coordinator responsible for their case.

The lack of accurate contact information in the VNS was confirmed by our audit. Eighteen percent of the 2,762 victim surveys we mailed to victims active in the VNS were returned to us as undeliverable mail. We were also told by staff and officials from VNS-participating agencies about problems they have encountered with undeliverable correspondence.

EOUSA officials acknowledged these issues, noted that they do not have the resources to follow up on initial notifications, and said that EOUSA was moving towards using the VNS website more than written notification letters. EOUSA officials also acknowledged that returned e-mail notifications was an emerging issue, and that they were in the process of establishing a protocol for identifying and getting information about undeliverable e-mail to participating agencies for action. Regardless of notification method, we believe that EOUSA should work with VNS-participating agencies to ensure that contact information in the VNS is as accurate as possible so that, at the very least, each victim receives an initial notification.

Archiving Data and Replacing Hardware

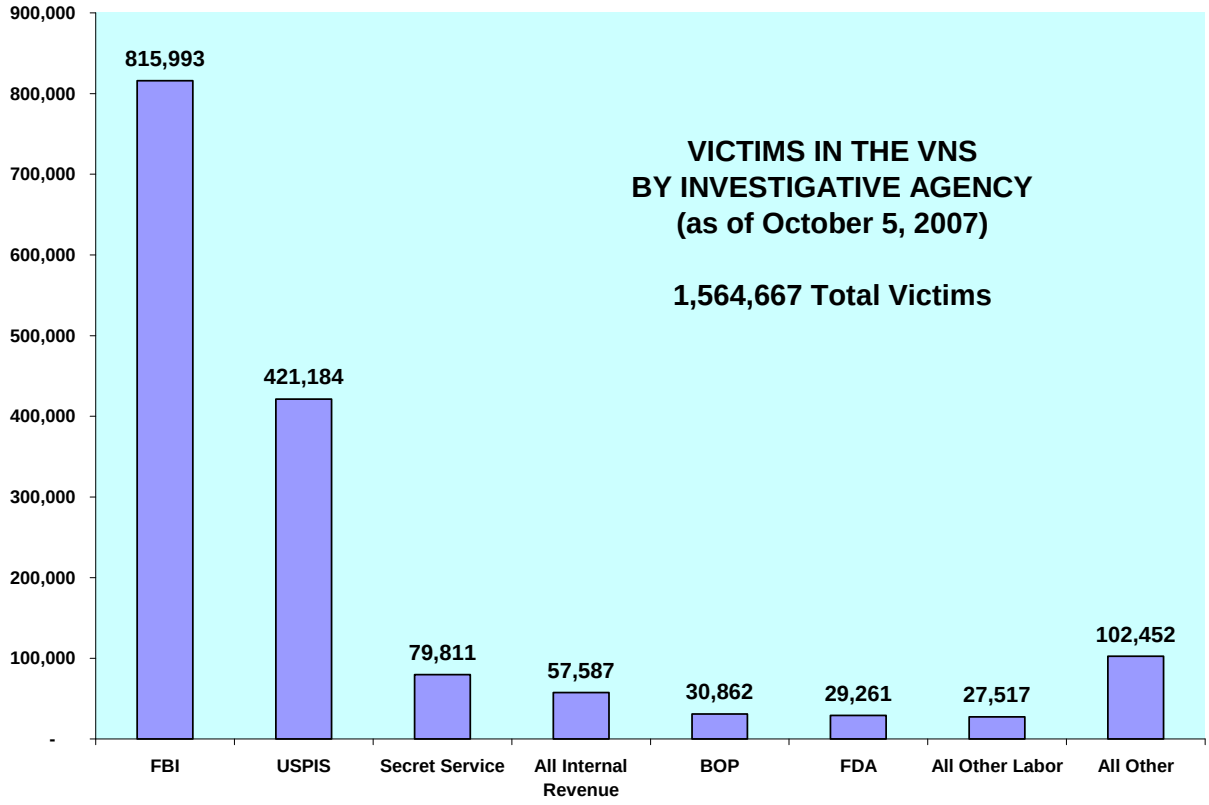
According to contractor personnel, as well as EOUSA's FY 2007 budget request, storage space on the VNS server has been filled to almost 80 percent of capacity. This has limited the speed at which data can be accessed and has become a bottleneck in the system. Additionally, much of the VNS's equipment is coming to the end of its useful life span and is in need of replacement. Although the VNS contract requires the contractor to archive VNS data periodically based on specific criteria, no VNS records have ever been archived and there are no current plans in place to do so.

During our audit, we discussed these issues with EOUSA and, in August 2007, EOUSA officials informed us that they plan to replace the existing equipment with new equipment that will resolve the capacity issue and the need to archive or remove data from being accessible online.

Outreach to Other Federal Agencies

In addition to all USAOs, only the FBI, the USPIS, the BOP, and the DOJ Criminal Division connect directly to the VNS. However, all investigative agencies are mandated to perform victim notifications during the investigative phase. Therefore, those federal investigative agencies who do not participate in the VNS, such as the United States Secret Service (USSS) and the Internal Revenue Service (IRS), must provide victims information during the investigative phase of a case on their own. Once they submit cases to a USAO, however, the USAO then "takes over" the notification process via an upload of information to the VNS.

EOUSA officials stated that their outreach efforts have been focused on those agencies whose cases involve the most victims. As shown in the following graphic, the FBI and the USPIS, by far, have the most (79 percent) victims in the VNS.



Source: OIG analysis of VNS data

In response to our discussions regarding other agencies that could possibly connect with the VNS, EOUSA officials advised us of their plans to create a universal, web-based interface with the VNS that could be utilized by all investigative agencies. We believe that this interface would be a useful step towards consolidating victim notifications throughout the federal government.

In addition to information about the investigative phase of a case, the VNS also provides notifications of court events, such as a competency hearing being held or a guilty plea being entered.[6] However, data related to court events is maintained by the Administrative Office of the U.S. Courts (AOUSC). In order for this data to make it into the VNS, it must first be obtained from the AOUSC and then manually entered into the USAO case management system by personnel at individual USAO offices. It is then uploaded from the USAO case management system to the VNS. During the course of our audit, EOUSA officials informed us of a plan to create an interface by which AOUSC data could be electronically passed to the VNS, thereby eliminating the time-consuming data-entry process, with its propensity for human input error.

[6] A complete list of VNS notifications can be found in Appendix IV.

In August 2007, EOUSA officials provided us with a copy of a signed Memorandum of Agreement (MOA) between EOUSA and the AOUSC to develop an interface between the two systems, and noted that the agencies are working together to connect the systems.

VNS Project Management and Succession Planning

Since its inception, the VNS has been managed by a single project manager, an Assistant United States Attorney based in Kansas City, Kansas. EOUSA has no formalized succession plan to continue management of the VNS should anything happen to key personnel. After discussing this issue with EOUSA, EOUSA officials informed us that they are developing a succession plan that will address any contingency issues for VNS project management.

VNS Effectiveness

To gauge the effectiveness of the VNS in notifying victims of certain key events, we interviewed federal VNS users and Call Center personnel, used a VNS test user account to assess VNS services from a victim's perspective, and conducted a survey of victims considered to be active in the VNS, as well as a survey of victims who had been "opted-out" (deactivated) of the VNS.

For our survey of those victims active in the VNS, we mailed out 2,783 surveys and received 691 responses. We reviewed these responses and determined that 531 of the 691 responses we received were valid and could be used for additional analysis. For our survey of those victims who had been "opted out" of the VNS, we mailed out 489 surveys, received 58 responses, and determined that 44 of these responses could be used for further analysis.[7]

Overall, we found that many active victim survey respondents found the notifications to be understandable and useful to some degree. However, we identified areas in which we believe EOUSA could improve the services the VNS provides to victims.

[7] A more detailed description of our survey methodology for our survey of victims active in the VNS can be found in Appendix VII. Our survey methodology for our survey of "opted-out" victims can be found in Appendix VIII.

Victim Notifications

Twenty-five percent of the active victim respondents to our survey indicated that they did not know about the VNS or that they were included in the VNS as a victim, that they had no idea why they had received our survey, or that our survey was the first piece of correspondence they had received regarding the VNS. Moreover, according to the VNS data, these respondents had each been sent an average of 18 notifications, and the number of notifications sent to these victims ranged between 1 and 160.

These responses indicate that the VNS is not as effective as it could be at notifying victims of case events. A significant number of federal crime victims have no knowledge of the system and are not receiving notifications from the VNS. In addition to the statutory requirement that victims be notified of events that occur in their cases, we believe it also important that EOUSA ensure that victims: (1) are aware that they qualify as victims of a federal crime, (2) are aware that their personal information is contained within the VNS, and (3) have been afforded the opportunity to decide whether they wish to receive notifications of events that occur within their cases.

We spoke with EOUSA officials about this issue, and they acknowledged that there is no formal follow-up process to ensure that victims receive notifications from the VNS. However, these officials expressed the belief that performing follow-up on letters would be overly burdensome on participating agency personnel and noted that EOUSA was moving towards using the VNS website more than written notification letters.

We believe that the purpose of the VNS is not always fulfilled by simply ensuring that notifications are sent out. Rather, we believe it is incumbent upon EOUSA to seek to ensure that as many victims as possible receive notifications. We recommend that the EOUSA work with VNS-participating agencies to develop procedures for ensuring victim contact information is current and undeliverable correspondence is pursued to help ensure victims receive case-related notifications from the VNS.

The Victim Internet System

The Victim Internet System (VIS) is a web-based application that allows victims to have access to a subset of VNS data related to their case via the Internet. We evaluated VIS services using a test victim account and included questions about the VIS in our survey of victims active in the VNS.

Accessing the VIS

In response to our survey, only 98 of the 531 victims who returned valid responses indicated that they accessed the VIS to review their case information.[8] We believe that EOUSA should be concerned about this relatively low 18-percent usage rate, considering that EOUSA officials informed us on several occasions that they prefer that victims utilize the VIS to obtain case information and that they have attempted to encourage its use.

The majority of our respondents who indicated that they utilized the VIS found it at least somewhat easy to set up their VNS account. However, other respondents commented on difficulties with the process they encountered. Our own review of the VIS using our test victim account also identified certain aspects in the process that could be confusing for victims, including problems with terminology. We spoke with EOUSA officials about these issues, and they responded that they will work to explain VIS procedures in more detail for victims.

Ease of Navigation, Comprehension, and Usefulness

More than 80 percent of the survey respondents stated that navigating or locating information on the VIS was at least somewhat easy. Additionally, most respondents found the information on the VIS to be both comprehensive and useful.

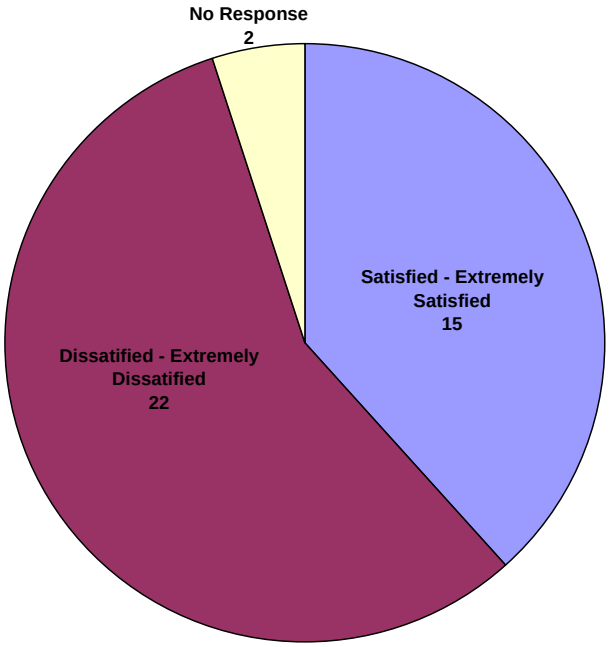
Restitution

On several occasions during our audit, EOUSA officials told us that personnel who worked with victims were often asked questions related to restitution.[9] We therefore included questions in our survey related to restitution information available on the VIS. We found that 40 percent of our respondents had accessed the VIS to obtain that information. Of those respondents, 57 percent were dissatisfied or extremely dissatisfied with the restitution information they received from the VIS. This analysis is shown in the following chart.

[8] We conducted all of our analyses related to the VIS on this universe of 98 respondents who indicated that they accessed the VIS to review case information.

[9] According to information on the VIS, restitution is defined as a court order directing the defendant to pay a fixed amount of money to the victim in order to compensate the victim for loss incurred as a result of the crime.

How satisfied were you with the restitution information you received?



Source: OIG survey of victims active in the VNS

Several provided additional comments about their dissatisfaction with the amount of restitution information available. We also used our test victim account to review restitution information provided in the VIS and found that the language for restitution in the VIS was not clearly written.

We discussed with EOUSA officials the possibility of providing more restitution information to victims on the VIS. While these officials initially noted that providing this information to victims is not required, in August 2007 EOUSA officials stated that they will clarify the information regarding restitution that is provided to victims on the VIS.

The VNS Call Center

The VNS Call Center consists of an automated, toll-free telephone response system, as well as operators who can provide case information to victims. The automated system generates computerized voice readings of notifications, while operators are able to provide victims answers to a limited number of questions and direct them to points of contact for additional case-related information. Call Center operators also provide information to federal VNS users.

We found that of the active victim survey respondents, 11 percent had called the toll-free number. We then conducted separate analyses on those victims who had utilized the automated response and those who had utilized the operator assistance.[10]

Call Center Automated Assistance

In total, we found that 37 (65 percent) of the 57 victims using Call Center services utilized automated assistance. As shown in the following chart, when we analyzed responses from these 37 victims, we found that 15 (41 percent) never or rarely received information, while 12 (32 percent) always or often received information.

Did you receive the information you wanted from the automated system?

Source: OIG survey of victims active in the VNS

As shown in the following chart, when we reviewed responses from these same 37 victims regarding the ease with which they were able to access information using the automated system, we found that most found the automated system at least somewhat easy to use.

[10] As part of our analysis, we found that 15 victims had utilized both automated and live Call Center assistance. We included these 15 victims in our analyses of each of these types of assistance in order to capture all of the victims utilizing a particular type of assistance.

How easy is it to access information through the automated system?

Source: OIG survey of victims active in the VNS

We also used our test victim account to evaluate the Call Center's automated assistance and identified some potentially confusing aspects, including uncertainty about what functions pressing certain buttons on the phone would accomplish. We also found that more case information was available to us on the VIS than via the automated assistance.

Overall, while the automated assistance appears to be relatively easy to use, it can prove challenging and does not always provide the desired information to victims, nor does it provide as much information as does the VIS. We believe it would be worthwhile for EOUSA to make the automated assistance more user-friendly for victims.

Call Center Operator Assistance

As noted earlier, the Call Center's operator assistance is able to provide victims only a limited amount of information. Specifically, according to Call Center staff, EOUSA has specified that Call Center operators can provide information on 10 case-specific areas. If victims require information outside of these areas, the Call Center staff tells them who to contact for further information.

Through our analyses, we found that 35 of the 59 victims who utilized Call Center services had utilized operator assistance. As shown in the chart that follows, when we analyzed the responses from these 35 victims, we determined that 16 of them always or often received the information they wanted from the live assistance.

Did you receive the information you wanted?
(from Live Call Center Assistance)

Source: OIG survey of victims active in the VNS

Despite this relatively positive response, 17 respondents who had utilized the assistance indicated that they were dissatisfied because: (1) the system lacked restitution information; (2) case or defendant custody information was not updated; and (3) the system did not contain, in general, enough information and assistance.

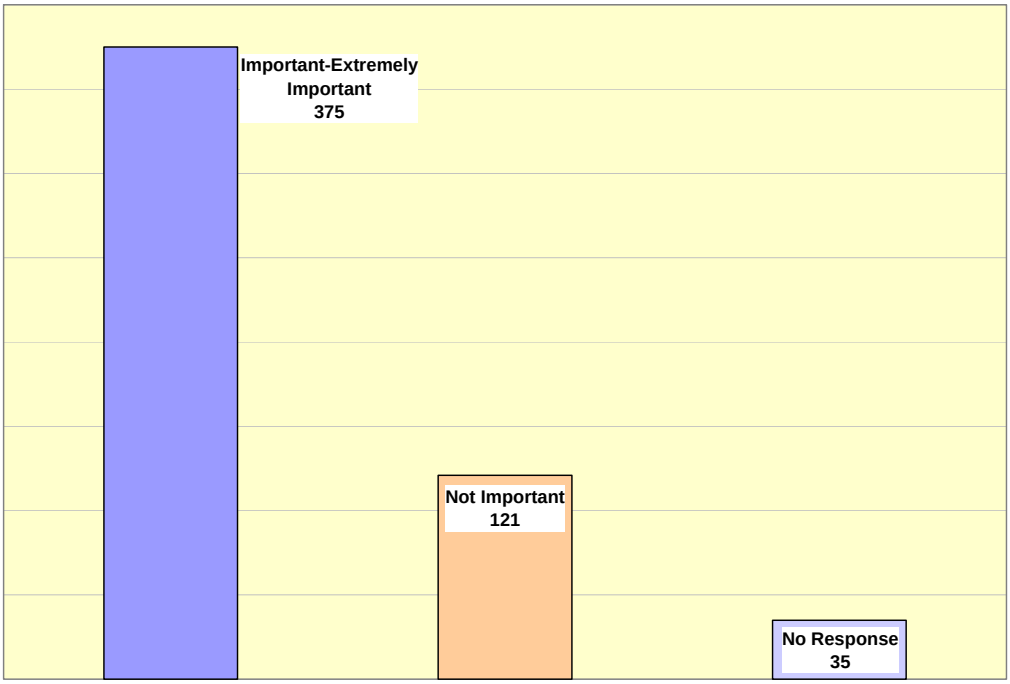
When we used our test victim account to evaluate the operator assistance, we identified several additional issues, such as the fact that a victim can only select to speak with a live operator at the beginning of a call. Specifically, if a caller does not immediately select that option (perhaps before the caller has received much information or had the time to develop questions), the caller must hang up, call back, and select to speak with a live operator at the outset of the call. We also found that the Call Center had only one Spanish-speaking operator on staff, who cannot cover every hour of every day the Call Center is in operation. This contradicts the VNS contract, which specifies that a victim must have the option of speaking directly with a Call Center operator to obtain case information in either English or Spanish.

We discussed these issues with EOUSA officials in June 2007. In August 2007, EOUSA officials informed us that they had notified the contractor of the requirement for a Spanish-speaking operator to be on duty during all Call Center operating hours. As a result, according to EOUSA officials, the contractor is now planning to add another Spanish-speaking operator to the Call Center.

Availability of Custody Status Data

In our survey of victims active in the VNS, we found that respondents considered custody status information to be very important. As depicted in the following chart, more than 70 percent (375 out of 531) of respondents indicated that knowing the custody status of the defendant was important to them.

How important is it for you to know the custody status (incarcerated or not incarcerated) of the defendant(s)/inmate(s) in your case?



Source: OIG survey of victims active in the VNS

The Attorney General Guidelines for Victim and Witness Assistance mandate that DOJ agencies notify victims of the release or escape of an offender or suspected offender. However, USAOs do not consistently enter defendant custody status information into the VNS during the prosecutorial phase. In addition, although the USMS maintains custody status information on offenders, it is not connected to the VNS and had not been approached to do so.

We discussed these issues with EOUSA officials, who agreed that they had not taken action to include in the VNS information from the USMS on defendant custody status. In August 2007, EOUSA officials advised us that providing custody status information to victims would be a priority and that they were coordinating with the USMS about this issue.

Victims No Longer Active in the VNS

Certain victims have been removed from an active status, or "opted-out" of the system. A victim can choose to be opted-out of the VNS or be opted-out by a federal user because of an invalid address or if the person is no longer considered to be a victim. While the VNS contains a field that records the reason a victim is opted-out of the system, it is not mandatory that a federal user populate this field when opting out a victim.

We analyzed VNS data provided by EOUSA and found that 164,493 victims were opted-out of the system between the VNS's inception in October 2001 and September 20, 2006. As depicted in the following table, when we further analyzed the data, we found that 32 percent of these victims had been opted-out with no reason given.

VICTIMS OPTED-OUT OF THE VNS
October 2001 to September 20, 2006

Opt-Out Reasons	Number of Registrants	Percentage
Contact Choice	4,144	3%
Invalid Address	79,597	48%
User Choice	28,486	17%
No Longer a Victim	17	<1%
No Reason Given	52,249	32%
Total	**164,493**	**100%**

Source: OIG analysis of VNS data

This large overall percentage of victims opted-out with no reason provided is troubling because there is no easy way to evaluate whether that victim was opted-out for a valid reason.

Survey of Opted-out Victims

As previously noted, in addition to our survey of victims active in the VNS, we also conducted a survey of opted-out victims. To maximize our response rate, we limited our universe to those victims opted-out of the VNS during the previous 2 full fiscal years prior to the survey, thus isolating 71,179 victims who were opted-out during FYs 2005 and 2006.

We developed a sample and sent our survey to 480 victims and received 58 responses, a relatively low 12-percent response rate. Overall, based on this relatively low overall response rate, including 203 surveys that were returned as undeliverable, our survey of opted-out victims did not provide clear evidence about why victims opt-out of the system.

VNS Information Security

During the course of our audit, we determined several attempted electronic break-ins to the VNS had occurred and that some recommended security patches for the system had not been installed because the patches had not been approved by EOUSA. After discussing these issues with EOUSA officials, we determined that the sensitive nature of the personally identifiable information (or PII) in the VNS – such as names, contact information, and social security numbers – as well as the possible consequences of failing to adequately protect it, warranted a more in-depth review of the VNS's information security. Therefore, the OIG contracted with outside auditors, Urbach, Kahn, & Werlin, LLP (UKW), to conduct an independent assessment to determine whether the VNS information security and privacy policies comply with government standards and established best practices.[11]

As a result of this assessment, we identified deficiencies with EOUSA's implementation of systems and communications protection controls, identification and authentication, website privacy, security measures, and web application controls. These deficiencies indicate that the sensitive information contained within the VNS was not adequately protected against loss of confidentiality and the integrity and availability of data was not appropriately ensured. Moreover, because of these issues the VNS may be susceptible to unauthorized use, access, or data modification.

Systems and Communications Protection Controls

Systems and communications protection controls prevent unauthorized and unintended information transfer between different elements within the same system. We identified weaknesses in transmission integrity and data validation.

Transmission integrity and data validation are used to check the completeness and accuracy of data entered into a system. We reviewed these controls for agencies that transmit data into the system and found that while EOUSA is encrypting data received from the USAOs, the DOJ Criminal Division, and the USPIS, it is not doing so for the FBI and the BOP. Additionally, EOUSA did not always ensure the completeness or accuracy of data files received from the BOP and the FBI. Because EOUSA is not performing these functions, it does not have the ability to detect or prevent

[11] In this section of our report, "we" and "our" refer to the auditors working under the direction of the OIG.

the alteration of transmitted data. When we spoke with EOUSA officials about this issue, they acknowledged these deficiencies and said they were currently discussing the implementation of complete session encryption for BOP and FBI data.

Identification and Authentication

Identification and authentication controls ensure that users' identities are verified before they can connect to the system. A system security plan, which is designed to provide an overview of the security requirements of the system and describe the controls in place, commonly contains this information for users. Moreover, these plans are necessary for certification, accreditation, and authorizing a system to operate. We found that the VNS system security plan contained inaccurate information and had not been updated with the correct procedural information, contact information, and process of authenticating users. This lack of an updated system security plan could result in an inaccurate or incomplete depiction of the VNS's system security and control environment, meaning that the certification and accreditation document is being approved based upon out-of-date information.

Website Privacy

Website privacy controls protect data collection and PII and include external linking policies. These controls inform users when they are about to visit a third-party website so that users know that they will no longer be protected by the privacy policies of the current site once they utilize a hyperlink to navigate to another website. We reviewed the VIS's external linking policies and found that the VIS does not provide such a disclaimer notification to users, meaning that victims who utilize the hyperlink may be unaware that differing privacy policies are in effect. DOJ policy specifies that a disclaimer statement informing users that they will no longer be protected by DOJ privacy policies must be provided.

VIS Web Application Controls Testing

Testing web application controls helps to identify vulnerabilities and risks that can result in the loss of confidentiality, integrity, and availability of data. We utilized commercially available software tools to evaluate the VIS's web application security and identified the following vulnerabilities:

- The VIS may allow manipulation within a web application, which can exploit security issues.

- The configuration of the VIS allows for the possibility that users could bypass the entry of usernames and passwords of linked web pages. As a result, individuals could gain access to unauthorized information.

- The application may be vulnerable to attacks that can allow malicious users to retrieve data or alter server settings.

- The VNS server configuration allowed for access to common default directories, which often contain exploitable vulnerabilities.

- The VNS uses a computer language, JavaScript, which has certain risks inherent to its use.

- The potential existed for unauthorized users to access web server administrative interfaces and thereby gain access to web server administrative functions.

- The VNS is susceptible to an attacker using web server software to access data in an unauthorized directory. Moreover, the execution of arbitrary commands and code by an attacker may be possible.

We consider the vulnerabilities found in the VIS web application controls to be significant because the system contains PII. We therefore recommend EOUSA take the necessary steps to improve its website security and eliminate these vulnerabilities.

The VNS Vulnerability Assessment

We also performed a vulnerability assessment to identify the security controls implemented for the VNS environment. We compared the VNS's current security controls to DOJ's standards and identified vulnerabilities within three areas.

- Unnecessary or Vulnerable Service – We found unnecessary or vulnerable services operating on the VNS, which if not properly secured or disabled, could be exploited to launch attacks against the system's infrastructure.

- Patch Management – We found that EOUSA did not always apply application and server patches in a timely manner.[12] Specifically, EOUSA had not applied several patches that had been available since 2002 and 2005, which, in essence, allowed a known vulnerability to continue to exist. This made the VNS susceptible to a disruption of its operations.

- Network Device and Server Security – Due to EOUSA's management of the VNS's device settings and configurations, the VNS may be susceptible to unauthorized use, access, or data modification of system configuration and password files.

Conclusion

Since VNS began in FY 2002, it has grown to contain information on more than 1 million federal crime victims. While creating such a system that was designed to provide notifications to so many individuals is an impressive achievement, we found certain areas in which VNS operations could be improved.

In terms of EOUSA's management of the VNS, we found that federal VNS users were generally satisfied with services provided by the VNS. However, weaknesses remain in the VNS Call Center's automated and Call Center assistance, the accuracy of data in the VNS, and the long-term plans for the future of the system. While EOUSA has taken proactive steps to address some of these issues after we brought them to its attention, other issues remain, and we recommend that EOUSA address these issues in the same manner.

We attempted to gauge the effectiveness of the VNS in notifying victims by conducting surveys of both active victims and those who have been opted-out of the system, as well as by using a test victim account to evaluate Call Center and VIS services. Our survey of those victims active in the VNS indicated that many of them found notifications to be understandable and useful to some degree. However, we identified areas in which VNS-related services could be improved. Most notably, a quarter of our respondents indicated they did not know about the VNS or that they were included in the VNS as a victim, that they had no idea why they had received our survey, or that our survey was the first piece of correspondence

[12] Patches are developed by software manufacturers following the identification of exploitable system security weaknesses. Patch management is the process of controlling the deployment and maintenance of interim software releases into a system's environment and is used to maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of the system's environment.

they had received regarding the VNS. Additionally, although EOUSA encourages victims to use the VNS website, only a small percentage of our respondents utilized it to obtain information about their cases. As with management of the system, EOUSA has already begun to implement corrective action to address these issues, and we recommend that it continue to do so.

Our information security review of the VNS identified several areas of concern, including weaknesses in systems and communications protection controls, identification and authentication controls, and web application controls. We believe that it is important that EOUSA work to address these vulnerabilities since the VNS contains PII on over 1 million victims of federal crimes.

As noted, according to EOUSA, it has already begun to implement corrective action to address some of the weaknesses we have identified. Additionally, to further assist EOUSA in the improvement of the VNS, we make 19 recommendations for EOUSA to improve the VNS, such as developing an interface to connect all relevant federal agencies to the VNS, formalizing long-term plans for the system and its management, improving certain facets of Call Center services, ensuring that a reason must be recorded in order to opt-out a victim from the VNS, and addressing the vulnerabilities identified during the information security review of the VNS.

THE VICTIM NOTIFICATION SYSTEM
TABLE OF CONTENTS

INTRODUCTION

In response to legislation directing federal law enforcement agencies to identify and provide certain services to crime victims, the Department of Justice (DOJ) developed the Victim Notification System (VNS), a computer-based system managed by DOJ's Executive Office for United States Attorneys (EOUSA). The VNS assists federal personnel in notifying victims of federal crimes of events occurring in the investigation, prosecution, and incarceration phases of their cases and provides victims various methods to access information regarding their cases.[13] The VNS came online in October 2001 and as of October 5, 2007, the VNS contained information on 1,564,667 victims.

Establishment and Funding of the VNS

The Victim and Witness Protection Act of 1982, the Victims of Crime Act of 1984, the Crime Control Act of 1990, the Violent Crime Control and Law Enforcement Act of 1994, the Justice for All Act of 2004, and the Attorney General's (AG) Guidelines for Victim and Witness Assistance established procedures to address the needs of victims of crime.[14] Each of these contains a directive to ensure that victims are notified of significant stages and procedural developments in the criminal justice process. Notification means keeping victims aware of the status of an investigation of a crime, as well as the subsequent prosecution, trial, incarceration, location, and custody status of the offender related to the crime.

On April 14, 1997, the Attorney General issued a memorandum that directed EOUSA to implement a comprehensive automated victim information and notification system as soon as possible. The Attorney General mandated that the system be available for use by investigative and prosecutorial components such as the Federal Bureau of Investigation (FBI), U.S. Attorneys' Offices (USAO), and the Federal Bureau of Prisons (BOP).

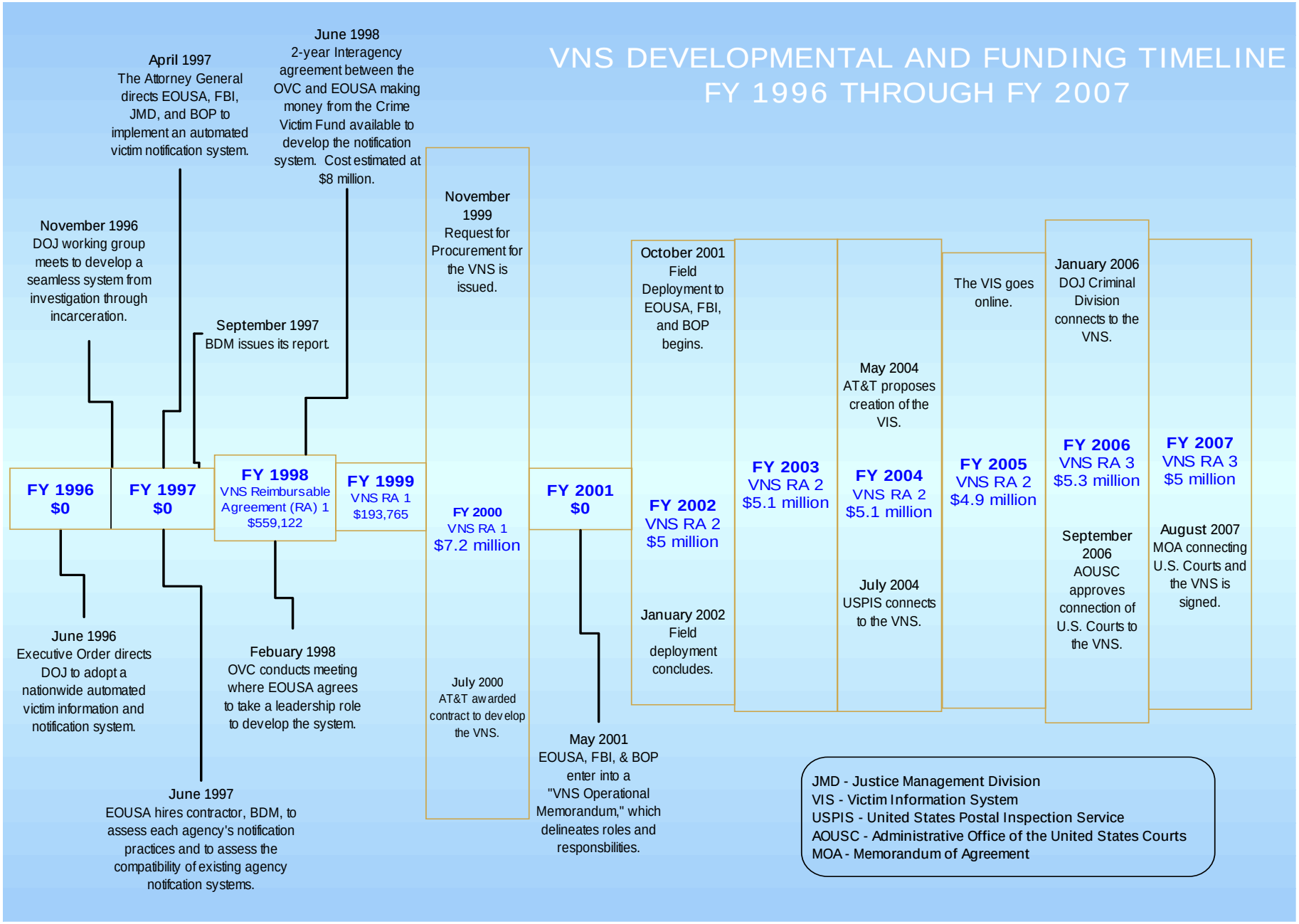
[13] A victim is defined in the VNS as an individual upon whom a criminal act is perpetrated and who is directly and proximately harmed as a result of a crime that is charged as a federal offense. Victims can decide to designate another person as their primary (alternate) contact to receive notification. This alternate contact is someone who can be reached in lieu of the victim, such as a friend, attorney, relative, or business associate of the victim, who also has an interest in the case.

[14] Additional information regarding this legislation can be found in Appendix II.

With funding provided by DOJ's Office for Victims of Crime (OVC), EOUSA managed the development of the VNS and actual field deployment began in early October 2001. The exhibit on the following page illustrates VNS's development and funding from fiscal year (FY) 1996 through FY 2007, highlighting a spike in funding in FY 2000, and a slight decline in funding levels since that time. Since work began on creating the system in FY 1998, the VNS has cost a total of more than $38 million.

According to EOUSA officials, the VNS received significantly more funding in FY 2000 than during any subsequent fiscal year to cover the initial development and implementation of the system. Officials stated that no funding was provided for the VNS in FY 2001 because the funding provided during the previous fiscal year had not been fully utilized.[15] Moreover, according to OVC officials, several reasons account for the slight decline in funding since FY 2004. Specifically: (1) the VNS is carrying forward the prior year's balance; and (2) funding for the Office of Justice Programs (OJP), of which the OVC is a part, has decreased.

[15] Additional information regarding VNS funding is found in Appendix III.


VNS DEVELOPMENTAL AND FUNDING TIMELINE
FY 1996 THROUGH FY 2007
November 1996
DOJ working group meets to develop a seamless system from investigation through incarceration.
April 1997
The Attorney General directs EOUSA, FBI, JMD, and BOP to implement an automated victim notification system.
September 1997
BDM issues its report.
June 1998
2-year Interagency agreement between the OVC and EOUSA making money from the Crime Victim Fund available to develop the notification system. Cost estimated at $8 million.
November 1999
Request for Procurement for the VNS is issued.
October 2001
Field Deployment to EOUSA, FBI, and BOP begins.
May 2004
AT&T proposes creation of the VIS.
The VIS goes online.
January 2006
DOJ Criminal Division connects to the VNS.
September 2006
AOUSC approves connection of U.S. Courts to the VNS.
August 2007
MOA connecting U.S. Courts and the VNS is signed.
FY 1996
$0
FY 1997
$0
FY 1998
VNS Reimbursable Agreement (RA) 1
$559,122
FY 1999
VNS RA 1
$193,765
FY 2000
VNS RA 1
$7.2 million
FY 2001
$0
FY 2002
VNS RA 2
$5 million
FY 2003
VNS RA 2
$5.1 million
FY 2004
VNS RA 2
$5.1 million
FY 2005
VNS RA 2
$4.9 million
FY 2006
VNS RA 3
$5.3 million
FY 2007
VNS RA 3
$5 million
June 1996
Executive Order directs DOJ to adopt a nationwide automated victim information and notification system.
June 1997
EOUSA hires contractor, BDM, to assess each agency's notification practices and to assess the compatibility of existing agency notifcation systems.
Febuary 1998
OVC conducts meeting where EOUSA agrees to take a leadership role to develop the system.
July 2000
AT&T awarded contract to develop the VNS.
May 2001
EOUSA, FBI, & BOP enter into a "VNS Operational Memorandum," which delineates roles and responsbilities.
January 2002
Field deployment concludes.
July 2004
USPIS connects to the VNS.
JMD - Justice Management Division
VIS - Victim Information System
USPIS - United States Postal Inspection Service
AOUSC - Administrative Office of the United States Courts
MOA - Memorandum of Agreement

How the VNS Works

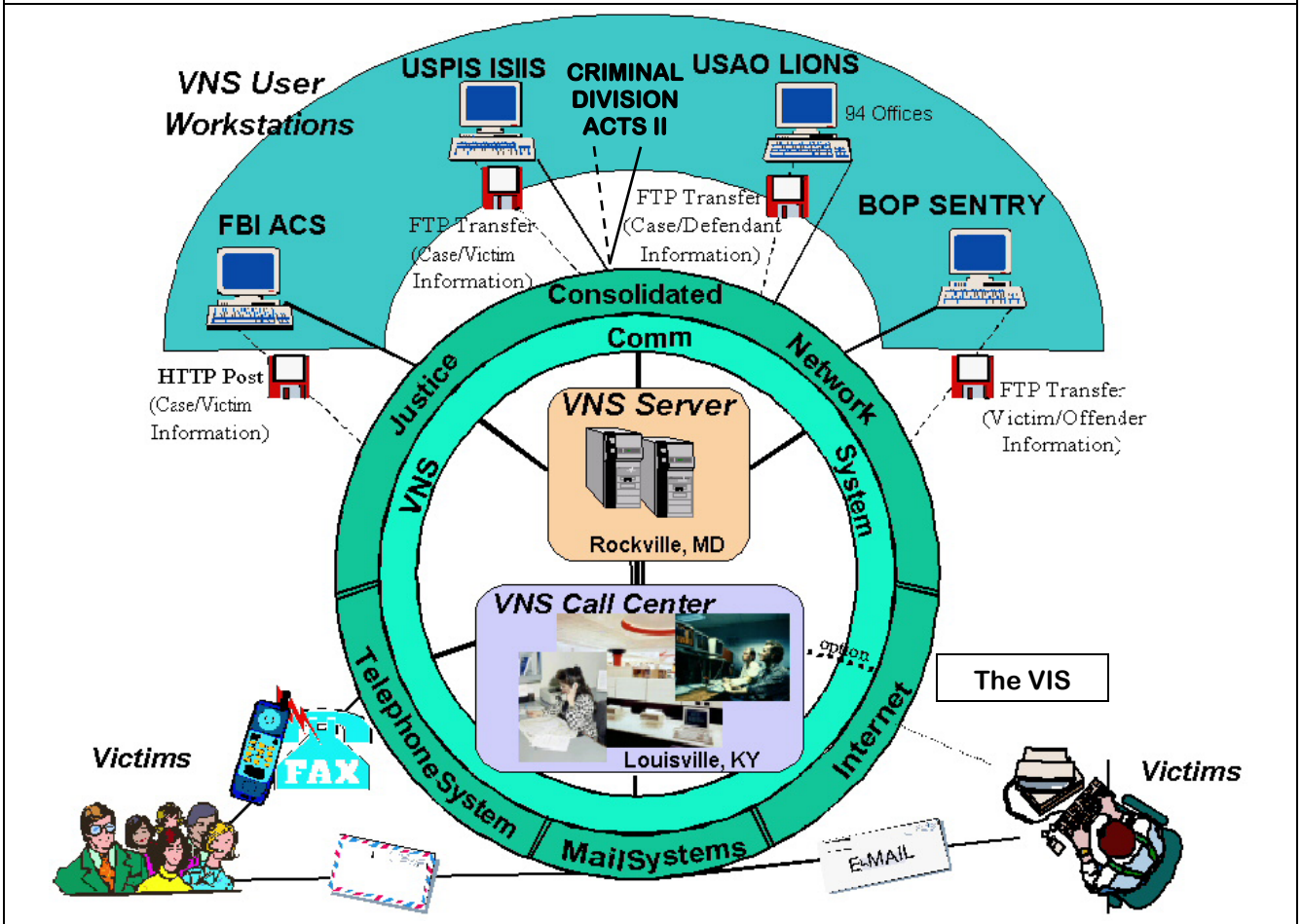
The VNS is a web-based application. The system hardware consists of a server, located at the Justice Data Center in Rockville, Maryland, as well as a Call Center facility and live back-up server in Louisville, Kentucky. The VNS receives data from automated case management systems at the FBI, USAOs, the DOJ Criminal Division, the United States Postal Inspection Service (USPIS), and the BOP. Specifically, the VNS receives daily downloads from the FBI's Automated Case Support (ACS) system, the USPIS's Inspection Service Integrated Information System (ISIIS), the USAO's Legal Information Office Network System (LIONS), the DOJ Criminal Division's Automated Case Tracking System II (ACTS II), and BOP's SENTRY system. Data transferred from the various systems includes case number; victim, defendant, and inmate information; court events; and custody status updates. Notably, some victim-related information that resides in the VNS is personally identifiable information (PII), such as the names, addresses, and, in some cases, social security numbers of victims of federal crimes.

Initially, the system consisted of the VNS, which federal VNS users accessed via a secure intranet connection, and the Call Center, which was used by both federal VNS users and victims of federal crimes. However, in FY 2004 the contract was modified to enhance VNS services by providing victims with Internet access to their case information. This resulted in the development of the Victim Internet System (VIS), which allows victims to have access to a subset of VNS data via the Internet. The VIS database server, in which the users' encrypted information is stored, is also located at the Justice Data Center.

Federal VNS users who specialize in dealing with victims and victim issues, such as FBI Victim Specialists and USAO Victim/Witness Coordinators, access the VNS to manage the information that relates to cases in the control of their agency. Victims of federal crimes utilize VNS services to obtain information on their related cases. Specifically, victims in the VNS are notified of case events by letter, e-mail, facsimile, or telephone when a particular event in a case occurs.[16] These victims can also obtain information at any time by calling the VNS Call Center or by accessing the VIS. The following graphic illustrates how the various component systems feed into the VNS, as well as how victim users of the system obtain case-related information.

[16] A list of all events that require notification is found in Appendix IV.

INFORMATION FLOW IN THE VNS



Source: VNS User Manual and the DOJ Criminal Division

Victim Notifications

In the VNS, a "notification" is a communication from the federal government to a victim, prompted by a particular event in the case. Events that prompt a notification to victims are referred to as "notifiable." When such an event occurs in a case, the identified victim in that case is notified via the VNS by a variety of means, such as letter, facsimile, e-mail, or telephone. Only victims and their alternate contacts who are "opted-in" to the system can receive notifications.[17] In addition to notification, a victim in the VNS can also obtain information on his or her case at any time by contacting the VNS Call Center or by accessing the VIS, which provides victims the capability to receive notifications, access information regarding

[17] "Opt-in" is the status of a victim or contact allowing them to receive notification and access the VNS Inbound Phone Line and Internet web page. Throughout the report we also refer to these victims as "active" in the VNS.

their case, and update their personal contact information via the Internet. A victim generally receives notifications regarding the three phases of the federal criminal justice process: the investigative, prosecutorial, and incarceration phases.

Investigative Phase

The investigative phase consists of the time after a crime has been committed (or allegedly been committed) to the time a case has been accepted or declined by the USAO for prosecution. The FBI and the USPIS are the only federal law enforcement agencies that utilize the VNS to notify victims of events that occur during the investigative phase of the criminal justice process.[18] The FBI and the USPIS provide limited investigative case information and detailed victim information through an export of data from their agency case management systems into the VNS. FBI and USPIS personnel then use the VNS to create, approve, and generate seven different victim notifications, such as an initial notification informing a victim that a case is under investigation, informing victims of their rights under U.S. law, or notification that a case has been referred for state or local prosecution.

Prosecutorial Phase

The prosecutorial phase encompasses the time charges have been filed by the USAO to the time a defendant is sentenced. As with the FBI and the USPIS, USAOs and the DOJ Criminal Division export information from their automated case management systems into the VNS. This information includes case data, as well as defendant, charge, and court event records, from cases that are either linked to previously loaded FBI or USPIS cases or are new USAO or Criminal Division cases investigated by agencies other than the FBI or the USPIS. The USAOs and the DOJ Criminal Division have 90 different notifications that relate to a defendant and contain case-specific information, such as the charges filed, trial dates, custody status, and sentencing information.

Incarceration Phase

The incarceration phase consists of the time a defendant is sentenced until the time a defendant is released from BOP custody. If a defendant is convicted and then sentenced to serve time in a federal facility, he or she becomes an inmate and is transferred to BOP custody. BOP notifications are

[18] Other federal criminal justice agencies, such as the Bureau of Alcohol, Tobacco, Firearms and Explosives, and the United States Secret Service, provide investigative phase notifications to victims without using the VNS.

created when data is received from BOP's SENTRY system. BOP personnel then use the VNS to create, approve, and generate 22 various types of notifications to victims, such as information related to defendant release, escape, or death.

VNS Oversight

In late 1999, the Deputy Director of EOUSA designated an Assistant United States Attorney (AUSA), located in Kansas City, Kansas, to assume program management responsibilities over the VNS. Since then, this project manager has been detailed to work full-time on the VNS and has held this position while physically remaining in the USAO in Kansas City. The project manager reports to EOUSA through the Office of Legal Programs and Policy.

In addition to the VNS Project Manager, additional program management responsibilities are to be carried out by various groups, including the VNS Executive Committee and the VNS Working Group. The VNS Executive Committee consists of senior-level management from EOUSA, the DOJ Criminal Division, the FBI, the BOP, the OVC, and the USPIS. The Executive Committee meets once a year to discuss financial issues, review system events from the previous year, and consider planned changes for the upcoming year. The VNS Working Group meets once a quarter and consists of representatives from EOUSA, the FBI, the DOJ Criminal Division, the BOP, and the USPIS. The purpose of the VNS Working Group is to review all proposed system changes and enhancements, implement its priorities, and provide input on any issues with the daily operation of the VNS.

OIG Audit Approach

The objectives of this audit were to determine if:

(1) EOUSA has effectively managed the VNS, including overseeing the contractors, ensuring the accuracy of data in the system, and planning for the future;

(2) The VNS is an effective tool for victims of crime; and

(3) The VNS is properly secured to prevent unauthorized use, access, and data modification.

To accomplish our audit objectives, we conducted more than 50 interviews with officials from agencies that are directly involved with the VNS, including officials from EOUSA, the DOJ Criminal Division, the FBI, the BOP, the USPIS, and the OVC. We also spoke with headquarters officials

from those agencies that do not directly participate in the VNS, such as the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Drug Enforcement Administration (DEA); the U.S. Marshals Service (USMS); the Administrative Office of the U.S. Courts (AOUSC); Immigration and Customs Enforcement (ICE); and the U.S. Secret Service (USSS) to determine their knowledge of the VNS, whether they were contacted about directly participating in the VNS, and why they do not participate. Additionally, we interviewed the contractor (AT&T Government Solutions), who manages the system, as well as the sub-contractor (Appriss), who manages the Call Center/Help Desk and back-up servers. We also reviewed internal documents from EOUSA, the DOJ Criminal Division, the FBI, the BOP, the USPIS, and the OVC. Those documents included planning materials, contracts, manuals, internal directives and policies, and financial reports. Moreover, we obtained and analyzed empirical data from the VNS and used this information to develop descriptive statistics on the number and types of victims in the system.

We conducted fieldwork in Chicago and Lisle, Illinois; Lexington and Louisville, Kentucky; Kansas City and Leavenworth, Kansas; and Kansas City, Missouri, where we interviewed 22 field personnel. At these locations we spoke with senior management and staff who utilized the VNS at the local USAO, BOP, USPIS, and FBI offices, and reviewed reports and files applicable to our review. In addition, at the FBI, we interviewed special agents who work cases with multiple victims. In general, the scope of our audit covered the period from FY 1998 through FY 2007.

Related to our first objective, we performed a limited review of the services provided by the contractor and sub-contractor, including Call Center operations; discussed the entry of information into the VNS with federal VNS users; reviewed data in the VNS and spoke with federal VNS users to determine if information in the system was accurate; and interviewed non-participating agencies to determine if outreach was performed and if the agencies were interested in participating directly with the VNS. Regarding our second objective to determine if the VNS is an effective tool for victims, we designed and deployed two surveys: one to victims who were active in the system and another to victims who were no longer active in the system.[19] We selected stratified, statistical samples of victims located throughout the world, to whom we sent the surveys.[20] We also reviewed other surveys conducted by EOUSA and BOP as well as conducted our own

[19] Copies of both of our surveys can be found in Appendices V and VI.

[20] Details of the surveys' scope and methodology can be found in Appendices VII and VIII.

testing of the VIS through use of a test victim account. In order to accomplish our third objective, we utilized a private auditing firm with experience in conducting information technology audits to perform an information security review of the VNS.

The results of our review are detailed in the Findings and Recommendations section of this report. Finding I discusses EOUSA's management of the VNS. Finding II reviews the VNS's effectiveness for federal VNS users and victims of crime. Finding III concentrates on the information security review portion of the audit. The audit scope and methodology are presented in Appendix I. Additional details on our review can be found in Appendices II through XI.

FINDINGS AND RECOMMENDATIONS

I. EOUSA MANAGEMENT OF THE VNS

We determined that government VNS users were generally satisfied with the work of the contractor and sub-contractor. However, EOUSA has not proactively assessed the accuracy of data within the VNS and a significant percentage of victim notifications are returned due to incorrect address information. For example, in our attempt to contact over 2,700 victims via mail, the correspondence that we sent to approximately 18 percent of these individuals was returned as undeliverable. Further, because data in the VNS has never been archived, storage space on the VNS server has been filled to almost 80 percent of its capacity, affecting both data access speed and performance of the system. While EOUSA has articulated its intent to resolve this issue, no schedule or written plans for doing so have been established. EOUSA needs to address other matters related to the future of the VNS, including following through on its plans to add additional government participants and establishing a succession plan for key program officials.

The VNS Contract

In FY 2000, EOUSA entered into a contract with AT&T to create the VNS. In addition to creating the actual information technology hardware and software for data entry and reporting, the contractor was required to establish and staff a Call Center to assist government and victim users of the VNS. It did so by sub-contracting with Appriss, Incorporated, to run and maintain the VNS Call Center. AT&T was also to supply training, Help Desk support, and system maintenance and enhancements. Once the system was developed, field deployment of the VNS began in October 2001. The VNS was fully operational by January 2002.

The VNS has a firm fixed-price contract, which was originally set to expire in September 2007, but which has been extended for 6 months.[21]

[21] The Federal Acquisition Regulation (FAR) System Subpart 16.202-1 states that a firm fixed-price contract provides for a price that is not subject to any adjustment based on the contractor's cost experience in performing the contract. This contract type places upon the contractor maximum risk and full responsibility for all costs and resulting profit or loss. It provides maximum incentive for the contractor to control costs and perform effectively and imposes a minimum administrative burden upon the contracting parties.

The annual cost to maintain the system is approximately $3.6 million. The primary VNS server is located at the Justice Data Center in Rockville, Maryland, with a mirrored back-up system located at the VNS Call Center in Louisville, Kentucky.

We reviewed the VNS contract and spoke with numerous federal VNS users to find out if they were satisfied with the system and the Call Center.

Satisfaction with Contractor Performance

To evaluate the performance of AT&T and Appriss in terms of contract fulfillment and services provided to federal VNS users, we conducted interviews with personnel at VNS-participating agencies. We also reviewed the results of an FY 2003 BOP survey of its employees who utilized the VNS.

The federal VNS users we interviewed stated that they were not aware of any problems that occurred with the administration or fulfillment of the VNS contract. They also said that contracting personnel were very responsive to users' requests. Federal VNS users also expressed satisfaction with the working relationship they had with the contractors.

The VNS Call Center

We determined that access to the Call Center is limited to DOJ-cleared staff and meets all the facility security requirements as described in the VNS contract. We toured the Call Center and spoke with the contractors and the sub-contracted personnel who worked there. The physical security of the facility generally appeared to be adequate to prevent access by unauthorized personnel.

According to the VNS operations manual, the primary purpose of the Call Center is to support: (1) victims by ensuring that information is captured and updated in the VNS and appropriate notifications are sent in an expeditious manner; (2) government agencies by providing system help and ensuring that information is transferred from external systems correctly; and (3) data and system integrity through the application of security, backup, and recovery processes. In addition to its duties as a Help Desk, Call Center employees assist federal VNS users with importing data for large cases that involve 300 or more victims.

To fulfill its mission, the Call Center maintains a toll-free telephone number that victims can call to obtain case information from either an

automated system or by speaking with Call Center staff.[22] As indicated in the chart below, data provided by the Call Center show 78,850 calls were placed in FY 2005. The number of calls decreased in FY 2006 to 63,959. Of these totals, 11,391 and 13,988 calls in FYs 2005 and 2006, respectively, required staff assistance from Call Center personnel.

Calls to the VNS Call Center

	FY 2005	FY 2006
Inbound	66,748	49,408
Operator	8,019	10,023
Help Desk	3,372	3,965
Abandoned Calls[23]	711	563
Total Calls	**78,850**	**63,959**

Additional Suggested Tasks for Call Center

According to BOP survey respondents and other government personnel we interviewed, they utilize the VNS Call Center for administrative purposes, as well as to address technical and access problems and to perform troubleshooting. The survey respondents generally had a positive opinion of the services provided by the Call Center, commenting that Call Center staff members were helpful, quick to respond, and open to suggestions for improvement. BOP officials did, however, state that they would like the VNS Call Center to notify victims of an escapee when the event occurs during BOP non-business hours, because the Call Center is open most of the time.[24]

Call Center personnel also commented that the automated ticketing system – called Tracker – for logging all calls they receive could be improved. Tracker is an internal database that is used by Call Center personnel to track calls from victims and federal VNS users, as well as to provide the VNS Project Manager with weekly reports on the status of Help Desk activity and system-related matters. However, the Call Center staff has to manually add specific information, such as callers' names, contact

[22] "Inbound" calls are calls to the automated toll-free number for which no live assistance was provided. "Operator" calls are from victims who dialed the toll-free number and selected "0" to speak with an operator. "Help Desk" calls are from personnel at VNS-participating agencies for application support.

[23] "Abandoned Calls" are instances where a caller hung up before completing the call or talking to a Call Center operator.

[24] The VNS Call Center is operational Monday through Friday, from 7:00 a.m. to 2:00 a.m.; Saturday from 7:00 a.m. to 12:00 a.m.; and Sunday 10:00 a.m. to 12:00 a.m.

information, and a summary of the problem. According to the VNS Project Manager, Tracker is functional for VNS purposes, but it is not a good interface for the Help Desk staff. Because the Call Center staff must manually create the ticket, it is very difficult to determine if all calls and issues are recorded and tracked.

The Call Center Manager explained that the Tracker system is rudimentary because all tracking activities have to be performed manually and the system cannot be easily searched. For example, in order to go back and check for specific information, a staff member has to review the entire list of calls, rather than zeroing in on a particular timeframe. Additionally, although a newer version of the Tracker software is available, Call Center employees said they are still using the original version.

Regarding a newer version of Tracker, during the audit a VNS official told us that Tracker is part of the record used by the contractor to provide weekly reports on the status of Help Desk activity and system-related matters. The VNS Project Manager stated that Tracker is an older system and is not as user-friendly to operate as are newer programs, but that it was being used due to a software compatibility issue. The VNS Project Manager also advised that the newest version of the Tracker software, called Front Range, will be installed during 2007.

We believe that upgrading Tracker to Front Range will help improve the quality of the contracted services provided, thus leading to an improvement in the service the VNS provides to victims. The ability to more easily analyze the content of user calls should allow EOUSA to identify and address existing problems that large numbers of victims might be having with the system, as well as allow EOUSA to forestall issues that may be in the developmental stage. However, the creation of the Tracker ticket should have some mechanism to ensure that tickets are created and that this task does not need to be performed manually.

In August 2007, an EOUSA official advised us that as of July 5, 2007, Tracker's upgrade to Front Range, which has greater report-tracking capability than Tracker, was complete. Moreover, EOUSA stated that it plans to implement Front Range's feature to automatically e-mail a caller upon the closing of a ticket. Additionally, a brief survey will accompany the e-mail to address any Call Center service problems experienced during operator assistance.

EOUSA's upgrade to Front Range demonstrates its willingness to follow through on its plans to improve the VNS. We believe it is important for the

agency to implement these plans for establishing the Front Range feature that will automatically e-mail a caller upon closure of a ticket.

Accuracy of VNS Information

In addition to ensuring that the terms of the VNS contract are fulfilled, EOUSA is also responsible for the content of the VNS. Victim information goes into the VNS when one of the various participating agencies enters the data in their own information systems and the data is uploaded to the VNS. After the initial victim record is created in the VNS through the upload process, any participating agency can enter additional information related to its cases directly into the VNS. Federal VNS users also have the option to remove a person from a case if that person is deemed to no longer be a victim.

According to the VNS Manual, when victims are added to the VNS from an agency information system, they are automatically associated with an investigative case, which, in turn, may be associated with one or many court cases. Victim records are thus automatically linked to all court cases associated with an investigative case, and if an event occurs for any associated case or defendant, each victim should be notified. However, federal VNS users can, when necessary, break the link between a victim and a specific court case or defendant if a victim is found not to be associated with that particular case or defendant.

The USAOs are responsible for creating all VNS records associated with agencies that do not participate in the VNS. For all non-participating investigative agencies, the USAO prosecuting the case creates the case and enters victim information into LIONS, the USAO case management system. Victim-related information is then uploaded electronically from LIONS to the VNS. However, in some cases with large numbers of victims, USAOs (as well as all other VNS-participating agencies) may enlist assistance from the VNS Call Center staff to create victim records in the VNS.

We interviewed federal VNS users to obtain feedback about the accuracy of VNS data. In addition, we assessed the controls and procedures in place to ensure the accuracy of information in the VNS.

VNS User Feedback

We asked users of the VNS at the FBI, the USPIS, the BOP, the DOJ Criminal Division, and USAOs about the accuracy of the data in the system. In general, users at these components considered VNS data to be accurate. However, a VNS Call Center analyst questioned the accuracy of

data related to court events. Specifically, problems occur when inaccurate court schedule information is entered into LIONS and is subsequently transferred to the VNS. In addition, BOP staff said that incomplete and inaccurate data is found in the information retained in the VNS. Additionally, responses to the 2003 BOP employee survey included negative comments about the accuracy of data in the system, a desire to have victim addresses updated, and claims that some data entered into the VNS by the FBI and USAOs was inaccurate or incomplete.

Undeliverable Correspondence

One measure of VNS data accuracy is the rate at which VNS correspondence is returned as undeliverable – that is, when the contact information for a victim is inadequate. We discussed with federal VNS users undeliverable mail and e-mail, along with policies and procedures for updating information in the VNS.

Interviews with most federal VNS users verified that there were no policies or procedures in place that required them to update victim contact information in the VNS when letters were returned. A BOP official stated that all returned notifications were forwarded to the USAO. At one USAO, we noticed a large number of notification letters sitting on the floor piled in bins. When we asked a Victim/Witness staff person about it, she stated that the letters had been returned because of inaccurate addresses and one of her responsibilities was to attempt to locate updated contact information.

USAO and EOUSA representatives stated that employees regularly use online databases to search for people by former addresses and social security numbers. They said that if a different address is located, the victim record is updated in the VNS. When a USAO receives undeliverable mail in large victim cases, the USAOs bundle the undeliverable envelopes and send them to the Call Center. The Call Center, in turn, modifies the victim records in the VNS to identify them as "opted-out" of the system, and then shreds the letters. According to the VNS Project Manager, this is done because the VNS lacks the resources to perform follow-up in such instances.

We also experienced problems with undeliverable correspondence in the course of conducting our victim surveys. When we attempted to contact 2,762 victims who were considered to be active in the VNS, 498 of our letters (18 percent) were returned as undeliverable.[25] The fact that

[25] Our attempt to contact victims in the VNS was performed as part of a survey related to victim satisfaction with the VNS. The results of our survey are conveyed in Finding II. The complete scope and methodology of this survey is contained in Appendix VII.

18 percent of the "active" victim records in our sample contained invalid addresses indicates that a significant number of victims may not be receiving notifications of case events.

We asked EOUSA officials what steps were taken for e-mails that were undeliverable. EOUSA acknowledged that returned e-mail notifications were a problem and that the problem was increasing in significance as the use of e-mail notification was rising. The VNS Project Manager further commented that EOUSA was in the process of establishing a protocol for identifying and getting information about undeliverable e-mail to federal VNS users for action.

In June 2007, EOUSA officials acknowledged to us that there was a problem with undeliverable correspondence, but noted their belief that it is the victim's responsibility to keep contact information up-to-date. Victims can update their information by various methods, such as via the VNS website or by contacting the USAO Victim-Witness Coordinator responsible for their case. According to the VNS Project Manager, federal VNS users are trained to make reasonable best efforts to find correct mailing addresses when correspondence is returned as undeliverable.

In response to our discussions with them on this issue, in August 2007 EOUSA officials informed us that they are researching approaches to implement a nation-wide procedure regarding undeliverable correspondence. The officials noted that this concern has become a higher priority for EOUSA and that this new procedure may be included in the next VNS contract.

VNS Procedures and System Controls

According to the VNS Project Manager, the accuracy of information in the VNS is largely dependent upon what was provided or entered originally by the participating agency. He added that there was no process for routinely checking the accuracy of victim files in the VNS and testing for accuracy of VNS data has not been performed. The FBI, the USPIS, and the BOP also have not tested the accuracy of the VNS data they entered.

An address is not required to enter a victim into the VNS. Rather, in order to add a victim to the VNS, the only required fields that must be entered are the victim's first name and last name or the victim's prefix and last name. However, in order for the victim to be sent an initial notification letter, there must be an address listed for the victim. If there is no address for the victim in the VNS when a letter is selected as a method of notification, the "initial" notification is left in a "pending" state and the victim will not be sent the initial notification letter until an address for that victim is

added to the VNS. When an initial notification is stopped for lack of a mailing address, the VNS alerts the responsible federal VNS user that a necessary notification was not sent due to the missing information. The VNS Manual directs federal VNS users to address these alerts. While the system does not have a control to ensure that federal VNS users respond to these alerts or confirm that the notifications are ultimately sent, it does leave the notification in a pending state to alert the user the notification has not been sent.

In sum, there are few internal controls to ensure the accuracy and completeness of information in the VNS. This means that victims whose contact information in the VNS is incorrect could be missing the opportunity to attend court events or be updated on defendant status. Although EOUSA believes it is the victim's responsibility to update all contact information, in our judgment, it is also EOUSA's responsibility to ensure that victim records in the VNS are as accurate as possible. We believe that EOUSA should work with other VNS-participating agencies to develop procedures for ensuring victim contact information is current and undeliverable correspondence is pursued to help ensure victims receive case-related notifications from the VNS.

In response to the concerns we raised, EOUSA officials explained that federal VNS users have the ability to generate a number of reports that allow for review of the data entered. At this time, the VNS does not automatically validate the mailing addresses of victims. EOUSA has reviewed the use of such automation and concluded that, at this time, such a process would require significant resources.

The Future of the VNS

In addition to reviewing the current status of information in the VNS, we also inquired about EOUSA's future plans for the VNS. We examined the VNS contract, which was initiated on August 1, 2000, and runs through September 30, 2007. The contract includes a clause allowing for a 6-month extension of services. According to the VNS Project Manager, the DOJ Justice Management Division (JMD) is responsible for procurement actions related to the VNS contract. JMD invoked the 6-month extension contract provision in June 2007 and EOUSA officials told us that they have provided necessary information to JMD for the next VNS contract.

We also examined EOUSA's long-term plans for the system, including the archiving of older data, replacing system hardware, outreach to additional federal agencies, and succession planning for management of the system.

Archiving and Storing VNS Data

The VNS contract states that the contractor will archive VNS data periodically. However, EOUSA and contract officials confirmed that VNS historical records have never been archived and they have no immediate plans to do so.

Contract employees, as well as EOUSA officials with whom we spoke, stated that all data entered into the VNS since it went online in October 2001 has been retained. According to contract employees, however, storage space on the server is an issue and the system needs to be upgraded for storage space. In its FY 2007 budget request, EOUSA confirmed that storage space in the system was an emerging issue. Specifically, the increased number of victims and notifications was pushing the current system to its physical capacity and this had limited the speed at which data could be accessed and become a bottleneck in the system. At the time of the budget request, the storage array as configured had 126 of its original 626 gigabytes of storage space remaining, meaning that the system was almost 80 percent full. This also meant that there was little room for future expansion for increasing data needs, and that the 6-year old technology used by the system is a bottleneck that limits data access speed.

In examining EOUSA's plans for archiving data, we also identified a concern with the established archiving criteria. The VNS contract states that records should be archived 36 months after a defendant is released from confinement. We asked EOUSA to provide a query to determine how many inmates in the VNS had been released prior to April 30, 2004, and we were told the VNS cannot readily obtain that information because it does not have a "released by BOP" field to make that determination. However, release of an inmate (such as permanent release, release to a halfway house or on furlough) are notifiable events.

In response to our discussions with EOUSA regarding our concern with VNS data never having been archived, in August 2007 EOUSA officials informed us that they plan to replace the existing equipment with new equipment in the near future. According to EOUSA officials, this will resolve the capacity issue and the need to archive or remove data from being accessible online.

System Hardware

In addition to issues related to archiving data, one staff person from the VNS Call Center expressed concern that VNS hardware is becoming outdated. We reviewed documentation related to this matter and found that

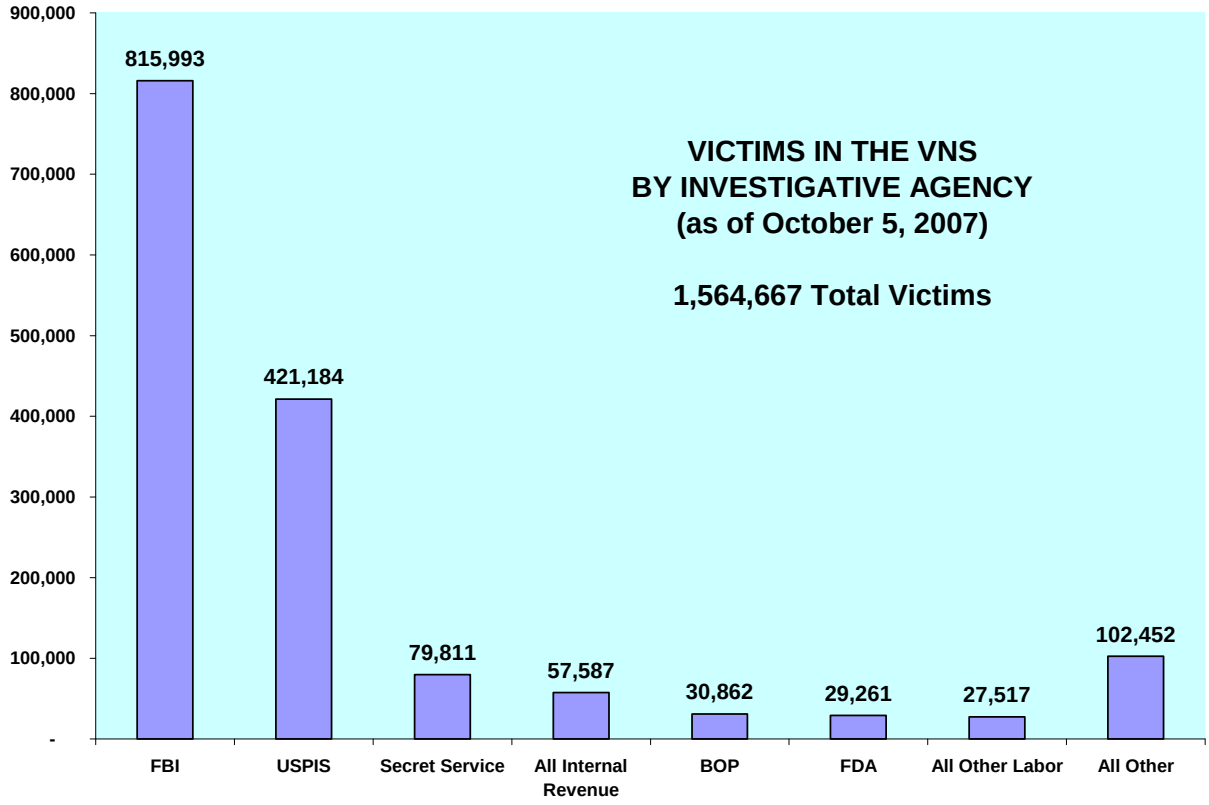
EOUSA's FY 2007 budget request stated that most of the equipment was 6-years old and coming to the end of its useful life span. A partial replacement of equipment was funded in FY 2006. However, more equipment needs to be replaced. The remaining equipment still in need of replacement includes the data storage system and the database servers. The replacement equipment and labor cost was projected at $700,000.

EOUSA Outreach to Other Agencies

Historically, EOUSA has coordinated with certain federal agencies to participate and use the VNS in carrying out their responsibilities to notify victims of case events. We examined these efforts as well as EOUSA's current efforts or plans to add new participating agencies.

At its inception, the VNS included the USAOs, the FBI, and the BOP. Since that time, the VNS has added two new agencies: the USPIS in FY 2004 and the DOJ Criminal Division in FY 2006. According to EOUSA, it is very expensive to modify the VNS by adding other investigative agencies' various case management systems. For that reason, EOUSA stated that it is not economically feasible to include all other agencies in the VNS because most investigative agencies have too few victims associated with their cases. Accordingly, EOUSA has focused its outreach efforts on agencies that have the most victims associated with their cases, such as the USPIS.

As of October 5, 2007, the FBI and USPIS were responsible for 1.2 million (79 percent) of the victims in the VNS. The number of victims, by agency, is shown in the following chart.



Source: OIG analysis of VNS data

Although not all investigative agencies participate in the VNS, all are mandated by statute to provide victims with information during the investigative phase.[26] We interviewed officials from several agencies that do not participate in the VNS: the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Drug Enforcement Administration (DEA); the United States Marshals Service (USMS); the Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE), and the United States Secret Service (USSS). According to representatives with whom we spoke from most of these non-participating agencies, they utilize their own resources to provide various forms of victim notification services similar to the type that the VNS was created to handle. We asked these agencies about their interest in the VNS and any contact they had with EOUSA officials about the system.

[26] Once these cases are forwarded to a USAO for prosecution, the notifications become the responsibility of the USAO and are then processed through the VNS.

- DEA officials stated that EOUSA approached the DEA when the VNS was first created, but the DEA declined to participate because the agency was worried about manpower, and issues related to system interface and security.

- An ATF official said that ATF special agents were interested in using the VNS, and he had requested information about the system from the VNS Project Manager. However, he stated that he did not receive a response to his inquiry and therefore the ATF had not had the opportunity to evaluate the benefits of using the VNS.

- USMS headquarters officials told us that EOUSA had not contacted the agency about participating in the VNS.

- The USSS does not have its own, or access to, any automated system to use for victim notification, and the USSS had never been contacted about joining the VNS. According to the USSS National Victim Coordinator, this is a concern because USSS cases are continually involving more victims. Therefore, the USSS official believed that joining the VNS was something that could be very helpful.

- The ICE official we interviewed stated that ICE had never been contacted about participating in the VNS and had no interest in doing so.

According to EOUSA officials, the agency is planning to create a universal interface that will allow all agencies with victim notification responsibilities to utilize the VNS through a web-based portal. According to EOUSA officials, creating this interface would eliminate the high cost of customized connections and the need for prioritizing outreach efforts. We agree with this plan and believe that it would eliminate the necessity for government agencies to duplicate the infrastructure for victim notification responsibilities.

Outreach for Court Event Data

The Administrative Office of the U.S. Courts (AOUSC) does not currently participate in the VNS, but EOUSA plans to connect the AOUSC's automated case management system to the VNS.[27] The purpose of adding the AOUSC to the VNS is to link public, court-docketed events directly with the VNS. This would eliminate the current need for USAO personnel manually to enter this information into LIONS so that it can be uploaded to the VNS. This manual process is time-consuming, increases the opportunity for human error, and increases the chances that court event information in the VNS may be incorrect, untimely, or never provided to the victim.

The proposal to connect the AOUSC to the VNS was approved by the AOUSC's Judicial Conference on September 19, 2006, pending funding to be provided by EOUSA. As of June 2007, EOUSA officials informed us that a draft Memorandum of Agreement (MOA) between EOUSA and the AOUSC for electronic VNS participation had been prepared and EOUSA was working on acquiring funding to develop the necessary interface. The estimated start-up cost for this endeavor was $800,000, and while EOUSA requested the necessary funding from the OVC, it did not receive sufficient funding in FY 2007's allocation to fund the AOUSC data changes. Therefore, EOUSA used its own appropriated funding to pay for the changes. The final step is for the AOUSC to develop software to extract its data to be sent to the VNS. The AOUSC estimates that developing this software will not be complicated and will cost $31,854. In August 2007 EOUSA officials provided us with a copy of the signed MOA between EOUSA and the AOUSC and noted that both agencies are working together to make necessary changes to the VNS for the connection.

Although the proposal has been endorsed by the AOUSC, it only addresses the development of the interface. According to EOUSA officials, they also will have to obtain approval from the Chief Judge in each judicial district to include court event information from that district in the VNS. Only then will all court event information flow directly from the AOUSC to the VNS. We believe that once the MOA is finalized and the interface is developed, EOUSA should work with the AOUSC to pursue the necessary

[27] The AOUSC is responsible for working with government agencies to coordinate and implement new legislation and procedures and to develop and support automated systems and technologies used throughout the courts. The AOUSC manages the federal courts' case management and electronic case files system, which provides the courts with enhanced and updated docket management; allows the courts to maintain case documents in electronic form; and gives each court the option of permitting case documents such as pleadings, motions, and petitions to be filed with the court over the Internet.

approvals from the Chief Judges so that all USAOs can benefit from the electronic sharing of court docket information.

VNS Project Management and Succession Planning

The VNS is managed by a single Project Manager. According to EOUSA officials, there are no formalized succession or contingency plans to continue the management of the VNS at the headquarters level should anything happen to key personnel. EOUSA's senior management informally discussed with us a contingency plan that could be implemented if the VNS Project Manager left. Yet, although it appears that EOUSA has considered how management of the VNS would proceed in the absence of the Project Manager, no formalized plan of action has been created. The amount of decision-making authority and system knowledge concentrated in the position makes the VNS Project Manager a critical person with responsibility for the VNS's uninterrupted day-to-day operations. We believe the importance of the service the VNS provides to millions of victims warrants a more concrete plan for the future. Thus, we believe it is important that EOUSA develop a formalized plan that could be implemented in the case of the current Project Manager's departure.

In addition, EOUSA does not have a formalized list of the future needs of the VNS, including enhancements to the system, upgrades to the system, replacement of outdated equipment, or growth of the system to meet the needs of federal VNS users and victims. At the beginning of the audit, EOUSA provided us with a list of future engineering changes, and since that time, we have been provided a current list of engineering changes for the VNS. Other than the engineering changes, however, EOUSA does not have any formalized long-term plans for the VNS. When we spoke with EOUSA officials about this in June 2007, they explained that all future plans for the VNS are limited to the short-term because of the upcoming expiration of the contract on September 30, 2007. However, in August 2007 EOUSA officials advised us that it has been developing a succession plan that will address any contingency issues.

Conclusion

We reviewed several aspects of VNS operations to evaluate EOUSA's management of the system. We found that federal VNS users were generally satisfied with the services being provided by the contractor and sub-contractor, and these users, on the whole, found the VNS Call Center to be helpful. However, we determined that limitations in the software used to track calls to the VNS Call Center prevented EOUSA from conducting detailed analyses of suggestions for improving the VNS. While EOUSA has stated

that it has addressed this issue with a software upgrade, we believe it is important for the agency to implement all of its planned enhancements.

We also found that there are few internal controls to ensure the accuracy and completeness of information in the VNS. Most importantly, this means that victims whose contact information in the VNS is incorrect or unavailable could be missing the opportunity to attend court events or be updated on defendant status. We attempted to contact over 2,700 victims as part of a victim survey, and in 18 percent of these instances, our correspondence was returned as undeliverable.

Further, VNS data, which dates back to October 2001, has never been archived and storage space on the VNS server has been filled to almost 80 percent of its capacity, a situation that has affected both data access speed and performance of the system. Also, although EOUSA has informed us that instead of archiving VNS data, it plans to expand the capacity of the system to alleviate the need for archiving, EOUSA has not yet established a formalized schedule or plan for doing so.

In addition, EOUSA has performed outreach to a limited number of federal agencies, selecting those agencies that have the most victims to keep informed, such as the USPIS. EOUSA is in the process of developing a universal interface that would allow all federal investigative agencies to upload victim information directly to the VNS. EOUSA is also currently in the process of establishing a connection between the AOUSC and the VNS, which would allow court information to flow directly to the VNS, thus improving the accuracy of court-related data and reducing the amount of manual labor required.

Finally, there are no formalized succession or contingency plans in place to ensure continuity of the VNS if the Project Manager who directs the VNS leaves his position.

Recommendations

We recommend that EOUSA:

1. Develop a written plan to: (1) archive VNS data, which should include a schedule for the initial archiving, parameters for subsequent archiving, and the criteria it will utilize to determine the records ready for archiving; or (2) acquire new equipment that will resolve the capacity issue.

2. Ensure that it is utilizing the newer version of the Tracker software, called Front Range, to allow for a more user-friendly data extraction and reporting function. Further, ensure that Front Range's feature that automatically e-mails the caller upon the closing of a ticket has been enabled and is being utilized to the fullest extent.

3. Develop a universal interface for federal investigative agencies to upload data directly to the VNS.

4. Work with the AOUSC to develop the hardware to connect the VNS and the AOUSC, develop a plan to connect individual federal court districts to the VNS using this interface, and endeavor to ensure that all federal districts are connected to the VNS.

5. Work with VNS-participating agencies to develop and implement procedures for federal VNS users to ensure that victims' contact information is current and updated.

6. Develop long-range plans for the VNS and its management that include: (1) future software and hardware upgrades, (2) replacement of outdated equipment, (3) expansion of VNS server storage capacity, (4) a projection of enhancements needed to account for the future needs of government and victim users, and (5) a formal succession plan for VNS project management.

7. Work with VNS-participating agencies to develop and implement a nationwide procedure for addressing undeliverable correspondence and e-mail.

II. THE VNS's EFFECTIVENESS FOR VICTIMS

Overall, the victims who responded to our survey were generally satisfied with the VNS and indicated that they felt VNS notifications were useful and easy to understand. However, our survey identified areas where improvements in the VNS could be made. Most notably, 25 percent of our survey respondents indicated that they had not heard of the VNS prior to receiving our survey, had never received a notification, or were not aware that they were registered as victims in the VNS. Further, although EOUSA encourages victims to obtain case information through the VNS website, only a small percentage of our respondents actually utilized it. Accessing the VNS website can be confusing and some victims find it difficult to navigate. Moreover, a large number of victims who responded to our survey were dissatisfied with the amount of information available to them regarding restitution and believe that knowing the custody status of offenders is important. We also determined that government VNS users can change a victim's VNS participation status from active to inactive without recording a reason for doing so, and without notifying the victim. We identified a significant number of victims who have been opted-out of the VNS with no reason recorded.

Background

To assess the VNS's effectiveness and victim satisfaction with the system as a whole, we conducted surveys of both active and inactive users to examine their level of satisfaction with the VNS. Additionally, we reviewed a 2003 BOP survey of its own VNS users. We also conducted our own review of VNS services from the perspective of a victim active in the system. Specifically, we requested and were provided a test victim account that we used to access the VNS victim-user website, known as the Victim Internet System (VIS), and the VNS Call Center's automated and staff assistance.

VNS Active Victim User Satisfaction

Our survey of victims identified as being active in the VNS covered many different aspects of the system, including the notification process, use of the VIS, and interaction with the VNS Call Center. From a universe of 618,203 victims active in the VNS during FYs 2005 and 2006, we selected a

stratified sample and mailed out surveys to 2,762 victims. We received 691 responses for a 25-percent return rate. We reviewed these submissions and identified 531 valid responses upon which we conducted our subsequent analyses.[28]

Overall, we found that our victim respondents were generally satisfied with what is provided to them through the VNS and that they found VNS services, such as the Call Center and the VIS, relatively easy to use. However, we identified areas of concern in our respondents' knowledge of the VNS's existence, overall use of the VIS by victims active in the system, and information provided in the area of restitution.

Victim Notifications

In our survey, we solicited comments from victim respondents regarding notifications of case information from the VNS and found that 173 (25 percent) of the original 691 survey respondents indicated that they did not know about the VNS, had never received a notification, or were unaware of their status as a victim of a federal crime. Further, some of these respondents reported that our survey was the first piece of correspondence they believed they had received regarding the VNS, and thus they had no idea why they had received the survey.

The number and nature of these comments is troubling. Based upon our analysis, it appears that there are a significant number of federal crime victims who have no knowledge that their personal information is contained within such a government database. We are aware of the statutory requirements that victims be notified of events that occur in their cases (and, thus, require that their information be contained in the VNS). However, in addition to the legal requirement to include them in the VNS, it is also important that EOUSA ensure that victims: (1) are aware that they are victims of a federal crime, (2) are aware that their personal information is contained within the VNS, and (3) have been afforded the opportunity to decide whether they wish to receive notifications of events that occur within their cases.

In light of victims' comments, we reviewed notification data provided by EOUSA. According to EOUSA, at the time we deployed our survey each of

[28] Additional information on this survey's scope and methodology can be found in Appendix VII.

the 173 respondents had been sent between 1 and 160 notifications, with the average number of notifications sent being 18.[29]

The fact that a quarter of our respondents indicated they did not know they were victims, despite the fact that EOUSA indicated that the individual had been sent at least one notification, indicates that the VNS might not be as effective as possible at keeping victims informed of case events. These results are similar to comments from the 2003 BOP survey of its employees who utilized the VNS. According to that survey's results, BOP users noted that in large fraud cases many victims were surprised by the notifications. In other instances, BOP users reported receiving calls from victims who indicated that they did not understand why they were being contacted and did not know anything about the inmate referred to in the VNS notification that was sent to them.

We spoke with EOUSA officials about this issue and they acknowledged that they have no formal follow-up process to ensure that victims receive notifications from the VNS. In contrast to EOUSA, the BOP has formalized initial notification quality control procedures included in their policies and procedures for the VNS. According to BOP policies, BOP staff perform follow-up work subsequent to sending notification correspondence to victims by ensuring each victim receives the notification. If the victim's preferred method of contact is unsuccessful, BOP staff are required to follow up with a notification letter to the victim.

According to EOUSA officials, sending follow-up letters would be overly burdensome on federal VNS users, and EOUSA was moving towards using the VIS as an alternative to written notification. However, we believe that, because the purpose of the VNS is to notify victims, the responsibility to do so should not end with making sure notifications are sent. Further, because our survey also identified that relatively few respondents were actively using the VIS, we believe EOUSA should take steps to ensure that victims are receiving at least their initial notifications, including improving its efforts to update victim contact information and addressing undeliverable correspondence and e-mail.[30]

[29] The data on notifications sent includes information provided via numerous methods, including letter, e-mail, or posting on the VNS website, VIS.

[30] Information about victim use of the VIS, which we obtained through our survey, begins on page 31.

Understanding Notifications

The format of the notification letters sent to victims is standardized. Prior to February 2006, federal VNS users were able to edit the text and adjust the format of the notification letters. EOUSA removed this editing capability to ensure that all notifications sent to victims contained necessary, standardized language. Although federal VNS users can add additional information to a letter, they cannot alter the format to ensure that it fits with the specific case for which it is being sent.

During the course of our audit, we spoke with federal VNS users and the VNS Call Center about the notifications. Many noted that information in notifications became confusing and sometimes contradictory when various types of notifications were combined in the same letter, and that the standard templates allowed little room to change information to clarify or correct the letters. Some also believed that letters generated by the VNS are vague and impersonal and can be insensitive to victims. Moreover, Call Center personnel told us that 70 to 80 percent of victims who contact the VNS Call Center do not know why they have been sent these letters, and that the letters do not clearly indicate that recipients are receiving the correspondence because they have been identified as victims of a federal crime.

The VNS Project Manager told us the standard templates were created to ease the notification burden for federal VNS users and allow them more time to assist victims in other ways, such as FBI Victim Specialists who provide other social services directly to victims in the field. According to EOUSA officials, they are aware that changes to the standard letters have been requested, but they said that certain language is required and the information currently conveyed is designed to provide the required information in a brief and accurate manner. EOUSA officials also noted that they have revised the standard language of the notifications once, at the behest of and with input from government VNS users. Moreover, the current template allows federal VNS users to add as much additional text to any of the standard language as necessary to help clarify the event for the victims. EOUSA officials also stated that they will make constructive revisions to the standard language of the notifications as necessary to meet statutory notification requirements.

In light of this issue, we asked survey respondents to indicate how easy it was to understand the information provided in the notifications they received. As shown in the following table, more than 80 percent of the responses indicated that the notifications were at least understandable, while less than 20 percent indicated that they found the notifications difficult to understand.

How easy is it for you to understand the information in the notifications?			
Choices	Number of Respondents	Percent of Respondents	Grouped Percentages
Very Easy to Understand	119	26	82
Easy to Understand	120	26	
Understandable	134	30	
Difficult to Understand	51	11	18
Very Difficult to Understand	8	2	
Extremely Difficult to Understand	21	5	
Totals	453[31]	100	100

Source: OIG survey of active victims

Usefulness of Notifications

We also asked the respondents to our survey about the usefulness of the information provided in the notifications. As shown in the following table, we found that almost half (48%) of the 448 victims who responded to this question found notifications to be useful to some degree, while 69 of the 448 respondents (15%) indicated they were not useful.

[31] Out of the 531 overall valid responses to our survey, 453 respondents answered this particular question, while 78 did not. Thus, we excluded from the analysis depicted in this table the 78 survey respondents who did not respond to this question.

Overall, how useful was the information provided to you in the notification(s)?			
Choices	Number of Respondents	Percent of Respondents	Grouped Percentages
Very Useful	68	15	48
Useful	148	33	
Neutral	163	36	36
Not Useful	37	8	15
Not Useful at All	32	7	
Totals	448[32]	100[33]	100[33]

Source: OIG survey of active victims

The Victim Internet System

As previously noted, the VIS is a web-based application that allows victims to have access to a subset of VNS data via the Internet. To determine the effectiveness of the VIS for victims, we included questions about the VIS in our victim surveys. We also utilized our test victim account and conducted our own testing of the VIS to assess how easy or difficult it was to use.

In analyzing the completed surveys, we observed that only 98 of the 531 victims who returned valid responses indicated that they accessed the VIS to review their case information.[34] This 18-percent VIS usage rate may be of concern to EOUSA, as officials informed us on more than one occasion that EOUSA prefers and has attempted to encourage victims to utilize the Internet-based VIS instead of relying on written notifications or the Call Center.

Accessing the VIS

As shown in the following graphic, which depicts the frequency with which the 98 victim respondents indicated that they had accessed the VIS, 27 victims (28 percent) stated that they had not accessed the website since

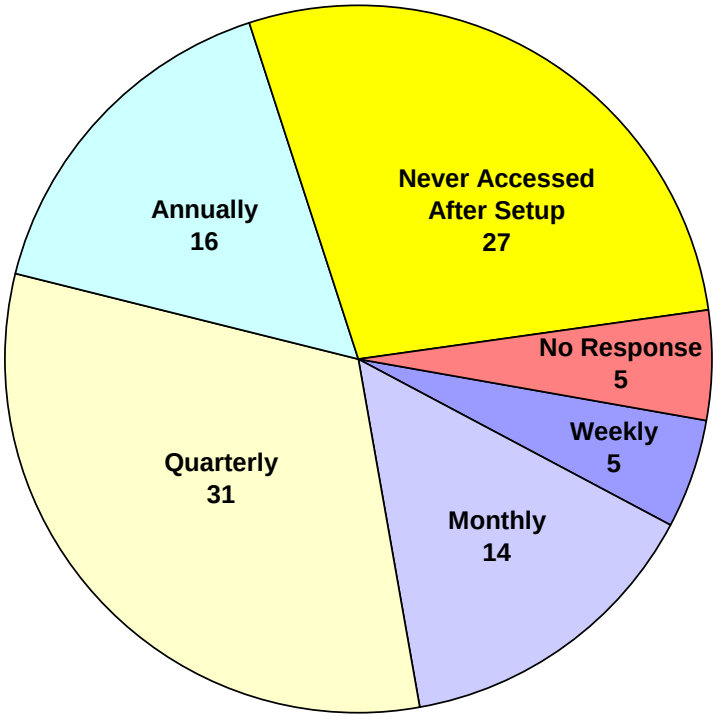
[32] Out of the 531 overall valid responses to our survey, 448 respondents answered this particular question, while 83 did not. Thus, we excluded from the analysis depicted in this table the 83 survey respondents who did not respond to this question.

[33] The numbers in these columns add up to 99 due to rounding.

[34] We conducted all of our analyses related to the VIS on this universe of 98 respondents who indicated that they accessed the VIS to review case information.

they first set up their account while 45 percent of the respondents used it monthly or quarterly.

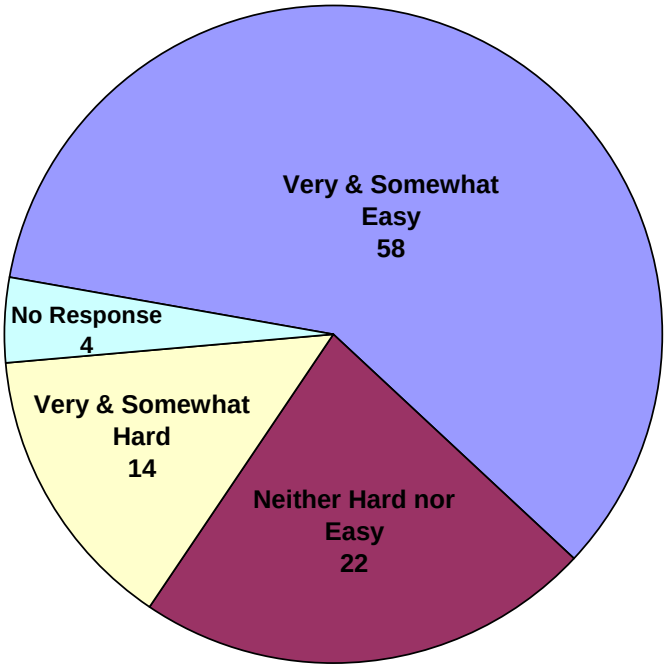
How often have you accessed the VNS website (VIS) for information?



Source: OIG survey of active victims

In our survey, we also asked victims how easy or difficult the process was to set up their website accounts. As shown in the following chart, the majority of the victims (58 out of 98) who accessed the website found setting up their user accounts to be easy while 14 victims found it somewhat or very difficult.

How easy or hard was the process to set up your VNS website (VIS) account?



Source: OIG survey of active victims

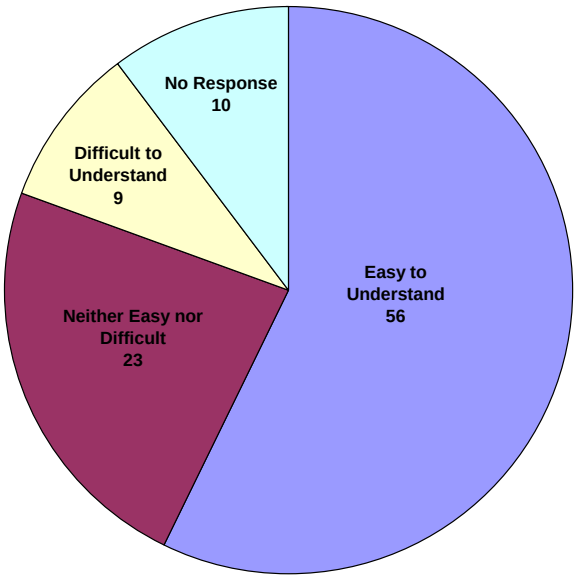
Despite this relatively positive overall response, some of the responding victims commented on problems they encountered with the process. Their comments included: "I tried to access the VNS website, but was unable;" "I received the VNS letter, but [the] letter has no VIN number or PIN number;" and "[I need] easier access to [the] website."

We also utilized our test victim status to set up a VIS user account. In doing so, we noted that the process includes steps that could be confusing for victims. Specifically, notification letters advise victims to use their Victim Identification Number (VIN) and Personal Identification Number (PIN) anytime they contact the Call Center or log on to the VIS. When we accessed the VIS, we were clearly requested to input our VIN. However, we were not clearly asked for the PIN. Rather, we were asked for our VNS Login ID (Password) to enter the website. EOUSA officials explained that the first time a victim logs into the VIS, they need to use their PIN as the VNS Login ID. Victims are then prompted to create a VNS Login ID for future access to the VIS. The originally issued PIN, however, remains active for access to the VNS Call Center. None of this was explained on the VIS website, nor in the letters. EOUSA officials stated that they will undertake a review of VIS access to improve these controls and work to explain this procedure in more detail.

Comprehension of VIS Data and Ease of Navigation

We also addressed the comprehensibility of information in the VIS in our victim survey. We asked victims how easy it was for them to understand the information on the website, and found that only 9 out of 98 respondents indicated that the information was difficult to understand, while the majority found the information easy to understand.

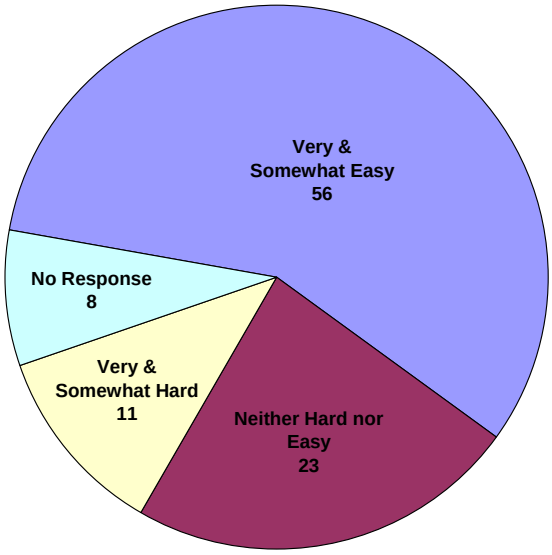
How easy was it for you to understand the information on the VNS website (VIS)?



Source: OIG survey of active victims

In addition, we analyzed our survey results to determine the ease with which victims navigated the VIS. According to the responses we received, only 11 of the 98 respondents found navigating the VIS to be difficult.

How easy or hard is it to navigate or find information within the VNS website (VIS)?

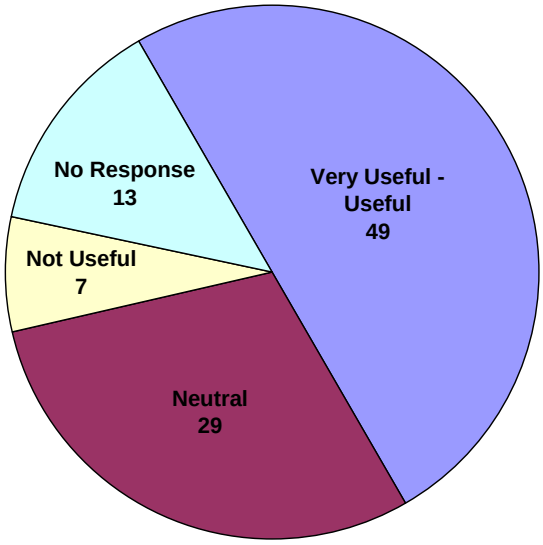


Source: OIG survey of active victims

Usefulness of VIS Information

One survey question asked victims if they thought the information provided on the VIS was useful. As depicted in the following graphic, one-half of the respondents found information on the VIS to be useful, while only seven victims indicated the information was not useful.

Overall, how useful is the information provided to you on the VNS website (VIS)?

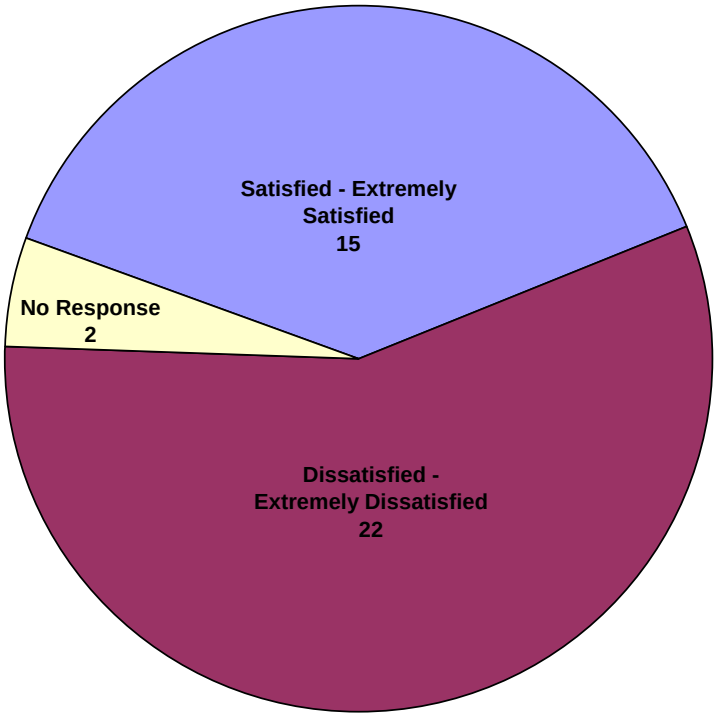


Source: OIG survey of active victims

Restitution

In our conversations with EOUSA officials, they stated that victims frequently asked about restitution.[35] In light of this, we included questions about the level of satisfaction victims had in regard to restitution information available on the VIS. Of the 98 respondents who utilized the VIS, 39 (40 percent) indicated that they accessed the website for information regarding restitution. Of those respondents, 56 percent were dissatisfied or extremely dissatisfied with the restitution information they received from the VIS. This analysis is shown in the following chart.

How satisfied were you with the restitution information you received?



Source: OIG survey of active victims

Many of the respondents who indicated that they were dissatisfied with the restitution information provided additional comments, such as:

- I received little notice, not restitution, not even updates. I had to send in victim information on more than 2 occasions – and I currently don't know if I'll get any of my money back.

[35] Restitution is defined on the VIS as a court order directing the defendant to pay a fixed amount of money to the victim in order to compensate the victim for loss incurred as a result of the crime.

- I seemed to get the "run around." There were no direct answers to my questions regarding restitution. The only thing that I was told was that they were proceeding with the investigation and I would be informed and updated. I haven't heard anything in a couple [of] years.

Because of the concern regarding restitution information noted by EOUSA and reaffirmed by the response to our survey, we used our test victim account to review restitution information provided in the VIS. We found that the information in the VIS related to restitution was not clearly written. Specifically, it was not apparent from the information available on the website whether or not our test victim was awarded restitution, and we believe that it would have been helpful if the VIS clearly indicated whether our case had restitution considerations. We discussed the restitution issue with EOUSA officials, who noted that informing victims that they are not receiving restitution is not required. However, EOUSA officials stated that they will change the language in the VIS "help" section to indicate that restitution information will only appear as that information is approved by the USAOs. Considering the importance that responding survey victims placed on restitution, we believe that the VIS could be improved by clearly indicating whether or not a case had restitution considerations, and we encourage EOUSA to make the described changes to language in the VIS to further clarify this matter to victims.

The VNS Call Center

In addition to the Internet-based VIS, a Call Center is maintained where victims can call a toll-free number and receive assistance via an automated response system or speak with an operator to receive information. While the automated system provides automated readings of notifications and gives victims the option to access other services available through the automated system, operators who staff the live assistance option can provide victims answers to a limited number of questions, direct victims where to call for further information, and provide information to federal VNS users.

We included questions about victims' experience with the VNS Call Center in our survey of victims identified as active in the VNS. Initially, we asked victims whether they called the toll-free number for Call Center assistance and found that only 59 (11 percent) of the 531 valid victim responses indicated that they had called the toll-free number, while 383 (72 percent) responded they had not done so. We then assessed the responses from the 59 victims who responded that they had called the toll-free number and determined that 29 indicated that they had terminated

their calls before receiving assistance for a variety of reasons.

We also reviewed our response data to determine what type of Call Center assistance our respondents had utilized: automated assistance, staff assistance, or a combination of both. As shown in the following table, we found that of the 59 respondents who had utilized the Call Center, 22 used automated assistance, 20 used staff assistance, and 15 utilized a combination of both.[36]

What type of assistance did you receive from the Call Center?		
Type of Assistance	Number	Percentage[37]
Automated	22	37
Operator	20	34
Both	15	25
No Answer	2	3

Source: OIG survey of active victims

In order to capture all of the victims utilizing a particular type of assistance, we included the 15 victims who indicated they had utilized both types of Call Center assistance in our separate analyses of automated and operator assistance.

Automated Assistance

As noted in the preceding table, of the 57 victims using Call Center services, 37 (65 percent) used automated assistance or a combination of automated and operator assistance. Additional questions answered by these 37 victims indicated that while 12 of them (32 percent) always or often received information, 15 (41 percent) responded that they never or rarely received information, and 5 (14 percent) only sometimes received information.

[36] Two of the 59 respondents who indicated that they had called the toll-free number did not respond to this question.

[37] The numbers in this column add up to 99 due to rounding.

Did you receive the information you wanted from the automated system?

Source: OIG survey of active victims

We also asked our survey respondents about the ease with which they were able to access information about their cases by using the automated system. As shown in the following chart, the majority of respondents – 21 – (57 percent) indicated that they found the automated system to be at least somewhat easy to use, while 11 respondents (30 percent) indicated that accessing information was not easy.

How easy is it to access information through the automated system?

Source: OIG survey of active victims

In response to our questions regarding what additional information the respondents would like to be able to receive from the automated assistance service, victims generally indicated that they would like current and more case information, such as restitution and custody status. Additionally, they would like to be able to easily gain access to a human operator from the automated assistance.

Similar to our evaluation of the VIS, we used our test victim account to assess the automated assistance provided by the VNS Call Center. We were able to access some of the automated features and identified areas that we believe could cause confusion for victims attempting to utilize these functions. For example, we noted some confusion in the numbers a victim needs to press in order to access certain VNS services. At the first prompt, the caller must press "2" to hear information in Spanish. Another prompt instructed the caller to press "2" at anytime during the message to return to the main menu. However, when we pressed "2," we were not directed to the beginning menu option. Rather, pressing "2" prompted an automated message that advised us to call the number on our initial notification letter if we needed assistance, and also advised us we could go to the website. Additionally, once we entered the automated system and made our first selection, there was no means for us to speak with an operator aside from hanging up and calling back.

Moreover, events were listed by defendant but not all historical events were provided, although this information was provided when we used the VIS. There also was no information available for any government-contact personnel working on a case. In addition, the automated assistance spelled out rather than said each defendant's name. As a result, it was a very long process to get to the defendant's information.

Overall, from the results of our survey as well as our own testing, we found that accessing the VNS's automated assistance could be challenging. The automated assistance was sometimes confusing, information available was limited in comparison to information available for the same case via the VIS, and obtaining the information could be a lengthy process. We believe that EOUSA should take necessary steps to improve the automated assistance system and make it more user-friendly for victims. At a minimum, users should be able to access an operator at any time during the call by pressing a single key, such as "0."

Call Center Operator Assistance

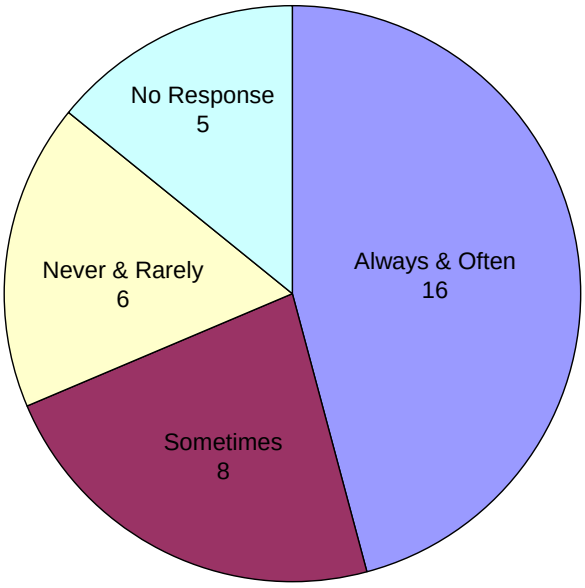
In addition to the Call Center's automated assistance, our victim survey included questions regarding the use of Call Center operator

assistance via its toll-free number. According to Call Center staff, they can provide contact information for further assistance and provide case-specific information related to 10 areas:

1) Current offender custody status
2) Current investigative status of case
3) Arrests made in the case
4) Sentencing information
5) Pleas made by defendant
6) Type of next court event
7) Date of next court event
8) Time of next court event
9) Inmate location
10) Inmate scheduled release date

As indicated in the chart on page 38, we found that 35 of the 59 victims who indicated that they utilized Call Center services also indicated that they had utilized the Call Center's operator assistance. For this analysis, we evaluated information provided by these 35 respondents who had utilized the operator assistance. As shown in the following chart, 16 respondents (46 percent) indicated that they always or often received the information they wanted, while only 6 respondents (17 percent) indicated that they never or rarely received the information.

Did you receive the information you wanted?
(from Live Call Center Assistance)



Source: OIG survey of active victims

We also solicited comments from the survey respondents about the Call Center's operator assistance. We found that 14 out of 29 respondents indicated that they were dissatisfied with the system because: (1) it lacked information regarding restitution; (2) it did not contain the updated information on the case or the custody of the defendant; and (3) the system generally did not have enough information and assistance.[38]

In response to these comments, EOUSA stated that the Call Center service level for victims is appropriate given the goals of the VNS project and the information available to individuals at the Call Center. Those goals are to provide victims the information required by the applicable statutes and the Attorney General Guidelines for Victim-Witness Assistance. EOUSA officials further explained that when victims have questions beyond the scope of VNS-related events, Call Center personnel direct the caller to the victim staff person of the agency currently involved with the case. This ensures that the victim speaks with someone who is familiar with the facts of the case and can provide the most up-to-date, accurate information, including information that is not available in the VNS.

We identified several additional issues when we performed our own evaluation of the Call Center's operator assistance. For example, we found that the only opportunity a victim has to speak with an operator occurs at the beginning of the call. If a caller does not immediately select that option (perhaps before the caller has received much information or had the time to develop questions), the caller must hang up, call back, and select to speak with a human operator at the outset of the call.

Another issue we identified is that, according to the VNS contract, a victim must have the option of speaking directly with a Call Center operator to be able to obtain case information in either English or Spanish. However, as of June 2007, the Call Center had only a single Spanish-speaking operator on staff, meaning that there are times each day when the Call Center is unable to provide this service to victims. According to EOUSA officials, subsequent to our discussion, they informed the contractor of the requirement that a Spanish-speaking operator must be on duty during all Call Center operating hours. As a result, the contractor is now planning to add another Spanish-speaking operator to the Call Center.

In sum, while some victim survey respondents commented on their displeasure with the Call Center's operator assistance, the majority of our

[38] Respondent comments on Call Center operator assistance can be found in Appendix IX.

survey respondents indicated that they received the information they needed. However, based on our testing, we believe EOUSA could improve the effectiveness of the Call Center's operator assistance by allowing callers to access a human operator at more points during a call, having a Spanish-speaking operator on duty during all hours of operation, and by allowing Call Center operators to provide more information to victims who contact them.

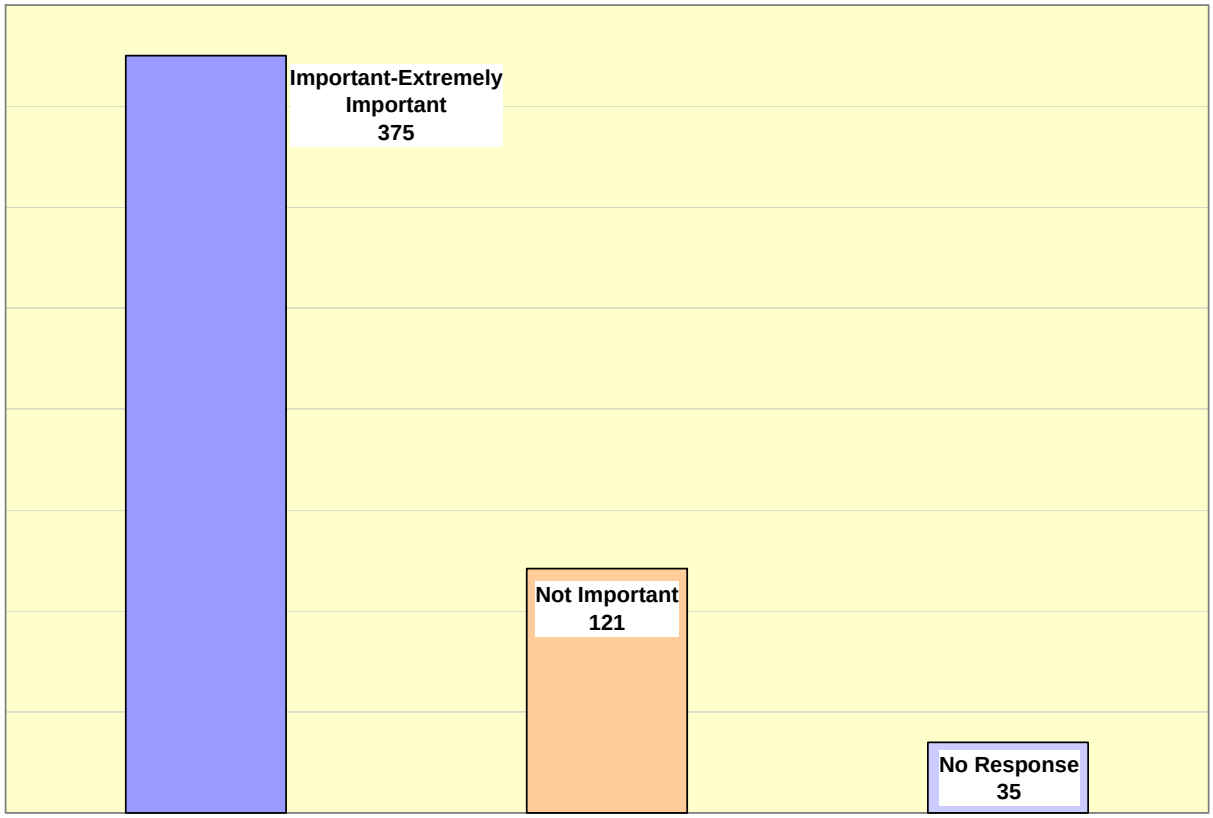
Availability of Custody Status Data

Access to defendant custody data is one of the most important features of the VNS. The Attorney General Victim Witness Guidelines direct agencies to notify victims of the release or escape of an offender or suspected offender. However, the USAOs do not consistently enter defendant custody status information into the VNS during the prosecutorial phase.[39] The VNS Project Manager stated that the USAOs do not consistently enter into the VNS custody status information on defendants during the criminal justice process and obtaining this information is not a top priority for the VNS.

We included questions about the importance of custody status in our survey of victims active in the VNS. As shown in the following graphic, 375 out of the 531 victims who responded to this question (71 percent) indicated that they considered knowing the custody status of the defendant to be "Extremely Important," "Very Important," or "Important."

[39] During the prosecutorial phase, a defendant may be released on bond or remanded into the custody of the respective U.S. Marshal to stand trial. Once a defendant has been convicted, sentenced, and remanded to a BOP correctional facility, the defendant moves to the incarceration phase and the provision of custody status information becomes the responsibility of the BOP.

How important is it for you to know the custody status (incarcerated or not incarcerated) of the defendant(s)/inmate(s) in your case?



Source: OIG survey of active victims

The USMS is the only entity that tracks the pre-sentencing custody status of federal defendants. We believe that it is important for the custody status of defendants in the prosecutorial phase to be provided to victims, as required by DOJ guidelines. We raised this issue with EOUSA officials in June 2007, noting that we were told by USMS officials that the USMS had never been approached by EOUSA to connect to the VNS. In response, EOUSA officials stated that funding an electronic interface between the VNS and the USMS was an issue, but requested contact information for the USMS officials we interviewed.

In August 2007, EOUSA officials advised us that providing custody status to victims would be a priority and that they had reached out to the USMS regarding this issue. According to EOUSA, the USMS is willing to provide custody status information to VNS. Further, EOUSA has provided direct appropriated money to fund any system changes that will be needed to accept data from the USMS.

Victims No Longer Active in the VNS

In addition to surveying active victims, we conducted a survey of victims who were no longer active in the VNS. These victims had once been active in the VNS, but had, for a variety of reasons, been "deactivated" and were now in an "opt-out" status.[40] We designed this part of the survey to determine whether the opted-out victims received an initial notification from a federal agency regarding the VNS and whether they subsequently chose not to receive notifications.

Victims may choose to "opt-out" of the VNS themselves or be opted-out when a federal VNS user chooses to stop sending them notifications. The VNS contains a field that offers one of four options that may be chosen to record the reason a victim is opted-out, as follows:

- *Contact Choice* indicates that the victim chose to be opted-out. Federal VNS users issue letters to these victims confirming they have been opted-out of the VNS.

- *Invalid Address* indicates the victim was opted-out due to an invalid address or letters that could not be delivered. Because of incorrect addresses there is no letter sent to alert the victim that they were opted-out of the system.

- *User Choice* indicates the federal VNS user has decided to opt a victim out of the VNS. However, federal VNS users do not send letters alerting victims that they were opted-out of the system.

- *No Longer a Victim* indicates that the federal VNS user determined the person who was originally notified of being a victim is no longer considered one.

Through our analyses of VNS data, we determined that 164,493 victims were opted-out of the system between the VNS's inception in October 2001 and September 20, 2006. We further analyzed the data to determine the reason these victims were opted-out of the system.

[40] According to the VNS Manual, "opt-out" indicates the status of a registered victim or contact who does not receive notifications and cannot access the VNS Inbound phone line or Internet web page. Although these victims are no longer considered to be active in the VNS, their names and information remain in the system.

VICTIMS OPTED-OUT OF THE VNS October 2001 to September 20, 2006		
Opt-Out Reasons	**Number of Registrants**	**Percentage**
Contact Choice	4,144	3%
Invalid Address	79,597	48%
User Choice	28,486	17%
No Longer a Victim	17	<1%
No Reason Given	52,249	32%
Total	**164,493**	**100%**

Source: OIG analysis of VNS data

We are concerned with the high number of victims identified as opted out due to invalid address information. This number is in addition to our other findings related to undeliverable mail and incorrect contact information. We believe that these opted-out victims with invalid address information are further evidence that EOUSA needs to improve its efforts to maintain up-to-date contact information, as recommended in Finding I.

We are also concerned with the high percentage of victims opted out of the VNS with no reason given. We discussed this issue with EOUSA officials, who confirmed that it is not mandatory to include in the VNS the reason a victim is opted-out. We believe that because there is no requirement for recording why someone was removed from the VNS, there is no easy means available to review a record to ensure that the victim was opted-out for a valid reason.

To maximize our response rate from those victims more recently opted-out of the system, we identified 71,179 victims who were opted-out of the VNS during the 2 full fiscal years prior to our analysis – 2005 and 2006. As shown in the following table, 73 percent of these 71,179 victims were opted-out of the VNS due to an invalid address, while 10 percent were opted-out with no reason provided.

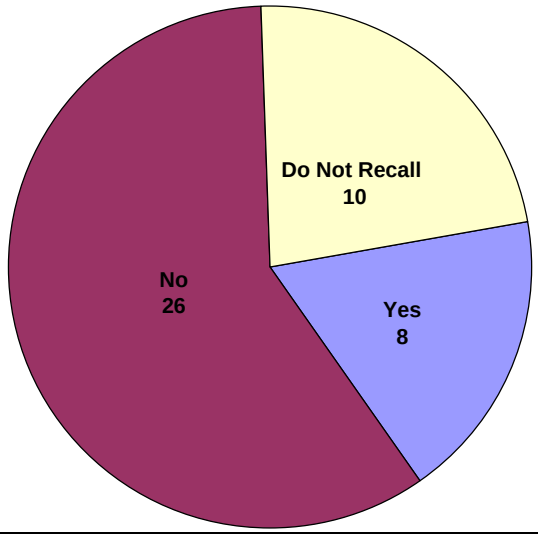
VICTIMS OPTED-OUT OF THE VNS October 1, 2004, through September 30, 2006		
Opt-Out Reasons	**Number of Registrants**	**Percent Value**
Contact Choice	1,580	2%
Invalid Address	52,029	73%
User Choice	10,548	15%
No Longer a Victim	56	<1%
No Reason Given	6,966	10%
Total	**71,179**	**100%**

Source: OIG analysis of VNS data

We then analyzed this data, selected a sample, and sent surveys to 480 victims.[41] We received 58 responses to our survey, resulting in a 12-percent response rate.[42] We then analyzed these 58 responses and isolated 44 out of the total that we considered to be valid.

We conducted analyses on these 44 responses and determined, as the following graphic shows, that only 18 percent (8 respondents) chose not to receive notification information.

Did you choose not to receive notification from the Victim Notification System?



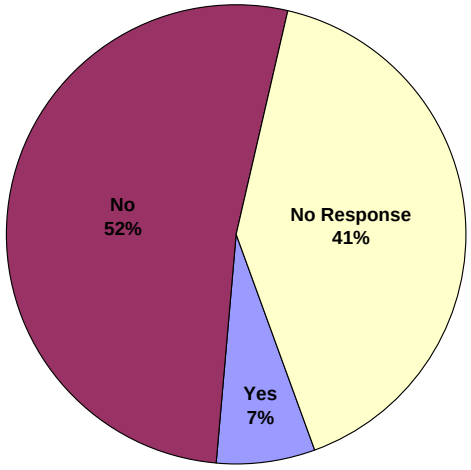
Source: OIG survey of victims opted-out of the VNS

[41] A detailed description of our opt-out survey's scope and methodology can be found in Appendix VIII.

[42] Of the 480 surveys that we sent out, 58 percent (280) were returned as undeliverable.

Furthermore, only three of our respondents (7 percent) indicated that they were informed by a federal agency that they were opted-out of the VNS and would no longer receive notifications.

If it was not your choice, were you informed by a federal agency that you would no longer receive notification?



Source: OIG survey of victims opted-out of the VNS

Overall, based on the high rate of undeliverable surveys, as well as the relatively low overall response rate, our survey of opted-out victims did not provide clear evidence about why victims opt-out of the system. However, we found that the majority of our respondents who did not choose to opt-out were not informed by a federal agency that they would no longer receive notifications from the VNS.

Conclusion

To gauge if victims are effectively being notified by the VNS of important case-related information, we conducted a survey of victims considered to be active in the VNS, utilized VNS services from a victim's perspective by using a VNS test user account, and interviewed federal VNS users and VNS Call Center personnel. In general, the victims who responded to our survey were satisfied with the VNS and indicated that they felt VNS notifications were useful and easy to understand.

However, we identified areas in which we believe EOUSA could improve the services the VNS provides to victims. For example, approximately 25 percent of our victim respondents were unaware of the VNS, had never received a notification, or were unaware of their status as a victim of a federal crime, despite having been sent at least one VNS

notification. These results indicate that many victims may not have been notified of case events.

Our interviews with government VNS users and Call Center personnel, as well as our own review of notifications provided to victims, found that notifications sent through the VNS did not always provide enough information to victims and that the standardized language within them can sometimes limit the effectiveness of the information provided.

From our survey, we determined that while the VNS website generally provides useful and understandable information to victims, the process and requisite passwords required to access it can sometimes be confusing and difficult. Additionally, we found that our respondents desired more information regarding restitution than what was provided on the website. Through our survey, we also determined that only a small portion of our respondents were using the VNS website – VIS – to obtain information about their cases.

We also surveyed victims about their use of the Call Center and performed our own testing of Call Center services to determine if the services it provides are effective. We found that the automated assistance was difficult to access, limited information was available to the caller, and the system was difficult to navigate and not user-friendly. We also found that the operator assistance option only allowed a person one opportunity to reach a human operator (and then only at the beginning of the call), a Spanish-speaking operator was not available during all hours of operation, and operators provided little information.

In addition to those victims considered to be active in the VNS, we also analyzed data on and conducted a survey of those victims who had previously been active in the system but were no longer active (referred to as “opted-out” in the VNS). We found that the VNS allows federal VNS users to opt a victim out of the system without recording a reason for doing so. According to data in the VNS, as of September 20, 2006, more than 160,000 victims had been opted-out of the VNS since its inception, with more than 50,000 of them having been opted-out with no reason recorded. We are concerned that because there is no requirement to list a reason, there is no easy means to determine if the decision to opt-out a particular victim was proper.

Our survey of victims opted-out of the VNS found that the majority of the individuals who responded to our survey indicated that it had not been their choice to be opted-out of the VNS and that most were not informed by a federal agency that they would no longer receive notifications from the VNS.

Recommendations

We recommend that EOUSA:

8. Improve the Call Center automated assistance to allow callers to reach an operator at any point during a call.

9. Follow up with the sub-contractor at the VNS Call Center to fulfill its requirement to have a Spanish-speaking operator available during all hours of operation.

10. Work with the USMS to ensure that the accurate custody status of defendants is available to victims utilizing VNS services.

11. Ensure that information regarding restitution is consistent throughout the VIS so that it is clear to victims whether restitution information is available to them.

12. Work with VNS-participating agencies to develop a requirement for federal VNS users to record a reason for opting a victim out of the VNS.

III. REVIEW OF VNS INFORMATION SECURITY

We evaluated the VNS's information security and privacy policies and identified various deficiencies, including EOUSA's implementation of systems and communications protection controls, identification and authentication, website privacy, and web application controls. As a result, the VNS may be susceptible to unauthorized use, access, or data modification. Because the VNS contains personally identifiable information (PII) for federal crime victims, such as names, contact information, and some social security numbers, EOUSA must improve its information security practices to help ensure that the data is appropriately protected against loss and misuse.

Background

During our interviews with VNS contractor personnel, we were informed that some recommended security patches for the system had not been installed because the patches had not been approved by EOUSA. In addition, during the course of our audit we were apprised of several attempted electronic break-ins to the VNS, which contains personally identifiable information (PII) from federal crime victims throughout the world. After discussing these security issues with EOUSA officials, we determined that the sensitive nature of this information (names, contact information, some social security numbers), as well as the possible consequences of failing adequately to protect it, warranted a more in-depth review of the VNS's information security. Therefore, the OIG contracted with outside auditors, Urbach, Kahn, & Werlin, LLP (UKW), to conduct an independent assessment in accordance with the Government Accountability Office's (GAO) *Generally Accepted Government Auditing Standards*.[43, 44]

Objectives, Scope, and Methodology of Review

We conducted an independent assessment to evaluate whether the VNS was properly configured to prevent unauthorized use, access, and data modification from sensitive and potentially vulnerable access points. We also determined whether information security control weaknesses exist surrounding the VNS's web interface; as well as to identify weaknesses

[43] In this section of our report, "we" and "our" refer to the auditors working under the direction of the OIG.

[44] The OIG regularly contracts with independent auditing firms to fulfill its responsibilities under the Federal Information Security Management Act.

associated with data collection, transmission, data storage, and PII. Further, we assessed the VNS's compliance with applicable federal information security policies and procedures for DOJ and EOUSA.

We performed a vulnerability assessment of the information security configuration of the VNS and tested web application security controls for the VIS. In order to identify whether the VNS complied with DOJ and federal privacy and information security policies, we performed interviews, on-site observations, and reviews of information security-related documents.

Overview of Information Security Controls Review Results

We concluded that the following information security control weaknesses exist within the VNS:

Information Security Control Areas	Function
Systems and Communications Protection	To prevent unauthorized and unintended information transfer via shared system resources.
Identification and Authentication	To verify the identity of users when accessing the system.
Website Privacy	To protect data collection and PII.
VNS Vulnerability Assessment	To determine the adequacy of security measures, identify security deficiencies, provide data from which to extrapolate the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
Web Application Controls	To identify issues related to vulnerabilities and risks associated with web applications.

We concluded that these deficiencies exist because EOUSA did not always fully develop, enforce, or formalize information technology (IT) security and privacy policies and procedures in accordance with current DOJ policies and procedures. We considered these weaknesses a moderate risk to the protection of the VNS and its data from unauthorized use, disclosure, loss, or modification in accordance with Federal Information Processing

Standards (FIPS) Publication (PUB) 199.[45] Specific details regarding findings identified during this review are discussed within the following sections.

Systems and Communications Protection Controls

The purpose of systems and communications protection controls is to prevent unauthorized and unintended information transfer between systems that share the same resources. We tested 12 control areas and identified weaknesses in transmission integrity and data validation.

Transmission Integrity and Data Validation

Transmission integrity and data validation are controls used to check for completeness and accuracy of data entered into a system. To ensure the integrity of transmitted data and its validation, encryption should be used for the transmission of interfacing data files.

The Department's Information Technology Security (ITS) standards require that checksums, hash totals, and record counts be used by applications to verify data integrity.[46] Components are strongly encouraged to have an automated means of detecting both intentional and unintentional modifications of data. Further, the Department's ITS standards require that communication channels are protected using FIPS-approved encryption modules.

We reviewed the transmission integrity and data validation documentation for five entities that transmit data into the VNS. Four were Department components – the FBI, the BOP, USAOs, and the Criminal Division. The fifth was the USPIS.

Although EOUSA is presently encrypting the transmission of data files received from the USAOs, the DOJ Criminal Division, and the USPIS, this is

[45] The FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* is required to be used by federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. The three levels of risk – low, moderate, and high – identify the potential impact on organizations or individuals should there be a breach of security. The FIPS PUB 199 defines the potential impact as moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

[46] A checksum is a type of redundancy check used to protect the integrity of data by detecting errors. Hash totals are used as an integrity check to identify files or verify their integrity. Record counts are used to ensure that records are not lost during transmission.

not the case for the BOP and the FBI. Moreover, we found that EOUSA did not always perform data validations as to the completeness or accuracy of data files received from the BOP and the FBI.

By not encrypting the transmitted data or performing data integrity checks, EOUSA does not have the ability to detect or prevent the alteration of transmitted data files. EOUSA acknowledged these deficiencies and is currently discussing the implementation of complete session encryption for BOP and FBI data. At the time of this report, both the FBI and the BOP stated that the necessary course of action was initiated in order to encrypt the data transmitted to the VNS.

Identification and Authentication

Identification and authentication controls are used to verify the identity of users when accessing the system. For this area, our review found a weakness in one of the six control areas tested.[47] Specifically, we found a deficiency regarding how system security information is reported in the VNS system security plan (SSP).

User identification and authentication is the process of uniquely identifying and authenticating users or devices before establishing a connection. Identification and authentication procedures are commonly communicated to the users in an SSP. A system security plan is designed to provide an overview of the security requirements of the system and describe the controls in place. SSPs are a key component of certification and accreditation packages and are relied upon by the designated approving authority to authorize a system's operation.

To maintain accreditation, the Department's ITS standards require each system to be reviewed annually. Further, system documentation should be modified to include any new security controls if they have been added post-development.

We found that the VNS system security plan had not been updated with the correct procedural information, contact information, and the correct process of authenticating users before establishing a network connection. We also identified that the document contained inaccurate information. For example, the VNS SSP states: "The VNS application will not blank the screen but will disconnect the user from the VNS after 10 minutes of

[47] The six control areas of identification and authentication we tested were controls for policy and procedures, user identification and authentication, device identification and authentication, identifier management, authenticator management, and cryptographic module authentication.

inactivity." However, we found that the VNS application is currently set to disconnect the user after a period of 20 minutes of inactivity.

Without an updated SSP, the depiction of the VNS's system security and control environment may be inaccurate or incomplete, which means that the individuals approving the certification and accreditation document are doing so based upon out-of-date information.

Website Privacy

Website privacy controls and data protection methods are enforced to protect data collection and PII. We identified a weakness in one of the seven control areas tested.[48] Our review revealed that the VNS's external linking practices failed to provide disclaimers or notifications to users when they are about to visit a third-party website. The intent of external linking notifications is to notify users that they will no longer be protected by the privacy policies of the current site they are visiting once they navigate to another website via a hyperlink.

The Department's *Guidance for the Implementation of Office of Management and Budget (OMB) Policies for Federal Agency Websites* states that websites should provide visitors an appropriate notification and a disclaimer statement when the individual leaves a Department website via a non-government link.

Occasionally, a federal VNS user will insert a hyperlink into the VNS that, when pursued, will send a victim using the VIS to another website that has additional information. For example, a third-party website might have social services information for victims. The VIS does not provide a disclaimer notification to users when visiting these third-party websites through a hyperlink. Without a disclaimer notification, VIS users may be unaware that differing privacy policies are in effect.

The VNS's VIS Web Application Controls Testing

The testing of web application controls is designed to identify issues related to vulnerabilities and risks associated with web applications. These vulnerabilities often result in the loss of confidentiality, integrity, and availability of data.

[48] The seven control areas of website privacy we tested were relevant content, approval of content, external linking, tracking mechanisms, persistent tracking mechanisms, disclaimers for tracking mechanisms, and privacy policy.

We utilized commercially available software tools to evaluate the VIS's web application information security controls.[49] We identified the following vulnerabilities:

- The VIS may allow manipulation within a web application, which can exploit security issues.
- The configuration of the VIS allows for the possibility that users could bypass the entry of usernames and passwords of linked web pages. As a result, individuals could gain access to unauthorized information.
- The application may be vulnerable to attacks that can allow malicious users to retrieve data or alter server settings.
- The VNS server configuration allowed for access to common default directories. Default directories often contain vulnerabilities that can be exploited over the web. Common default directories are installed during initial installation and all non-essential directories should be removed by the administrator and essential directories should be protected by authentication.
- The VNS uses JavaScript, a computer language used to create interactive websites and web applications, which has certain risks inherent to its use. For example, JavaScript may be able to scan a network, identify all web-enabled devices, and send attacks or commands to these devices.
- The potential existed for unauthorized users to access web server administrative interfaces. These interfaces are used by the website administrator to maintain the website and are usually not available to the public.
- The VNS is susceptible to exploits in which an attacker uses the software on a web server to access data in a directory prohibited for use by the attacker. Moreover, the execution of arbitrary commands and code by an attacker may be possible.

[49] See Appendix XI for the full details and results of web application testing. The test procedures were limited to the arrangements made with EOUSA, which required that non-destructive testing be performed. In other words, our testing could identify that a vulnerability existed, but we could not attempt to exploit that vulnerability to examine the effect of the weakness or any possible consequence of an external exploitation of the weakness.

The sensitive information contained within the VNS was not adequately protected against the loss of confidentiality, integrity, and availability of data. The vulnerabilities found in the VNS's VIS web application controls are significant because the system contains personally identifiable information for federal crime victims that includes names, contact information, and some social security numbers. Therefore, EOUSA should take necessary actions to improve its website security to help protect the identities of victims of federal crimes.

The VNS Vulnerability Assessment

A vulnerability assessment is the systematic examination of an information system that determines the adequacy of security measures, identifies security deficiencies, provides data from which to extrapolate the effectiveness of proposed security measures, and confirms the adequacy of such measures after implementation.

We performed a vulnerability assessment to identify the information security controls implemented for the VNS environment. We reviewed the VNS's current information security controls to determine whether they were implemented to adhere to the Department's standards. We identified vulnerabilities within the three areas described below.[50]

Unnecessary or Vulnerable Service

System services can be used to operate computer servers or trigger operating system functions. These services can pose serious security threats to the system and network if they are not secured. Further, unnecessary services should be disabled.

During the review of VNS information security controls, we found unnecessary or vulnerable services operating on the system. If not properly secured or disabled, these services could be exploited to launch attacks against the VNS infrastructure. For example, the VNS file transfer protocol (also commonly referred to as "FTP"), designed for the transfer of files remotely over large distances, was identified as an older version of this protocol. This version permits passing of user identification and password as well as session data in plain text without encryption. Allowing log-ins and passwords to pass between client and server in plain text makes them vulnerable to session high-jacking. Therefore, this service should be disabled and all transfers of files be done with encryption.

[50] See Appendix X for the full details and results of the vulnerability assessment.

Patch Management

Patch management is the process of controlling the deployment and maintenance of interim software releases into the system's environment. It is used to maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of the system's environment.

Patches are developed by software manufacturers following the identification of system security weaknesses that can be exploited. When systems' patches are not current, the risk posed by the weaknesses the patches were created to address is increased.

We found that EOUSA did not always apply application and server patches in a timely manner. Several patches that had been available since 2002 and 2005 had not been applied. In essence, by not applying the patches, EOUSA has allowed a known system vulnerability to continue to exist. As a result, at a minimum, the VNS is susceptible to a disruption of its operations. This disruption could be caused by a "Trojan Horse" - a destructive program that masquerades as a benign application before it is executed. The VNS may also be vulnerable to a buffer overflow, which occurs when a program or process tries to store more data in a temporary data storage area than it was intended to hold. This data can overflow into adjacent storage areas, corrupting or overwriting the valid data held in them.

Network Device and Server Security

Network device and server security refers to the management of device settings and configurations implemented in order to secure the system and network infrastructure.

By not implementing security standards and best practices to protect against common vulnerabilities, the VNS may be susceptible to unauthorized use, access, or data modification of system configuration and password files. Because of these vulnerabilities, VNS data that is being transmitted across the system may be intercepted and redirected to a person who is not authorized to receive the data. Additionally, an attacker could possibly interfere with system operations and cause the system to become inoperable.

Conclusion

We found that the sensitive information contained in the VNS may be susceptible to unauthorized use, access, or data modification. We identified deficiencies with EOUSA's implementation of systems and communications protection controls, identification and authentication, website privacy, web application controls, unnecessary or vulnerable system services, patch management, and network device and server security. These deficiencies exist because EOUSA did not always fully develop, enforce, or formalize IT security and privacy policies and procedures in accordance with current Department information security policies and procedures.

Because the VNS contains personally identifiable information for federal crime victims such as names, contact information, and some social security numbers, EOUSA must improve its information security practices to help ensure that the data is appropriately protected.

Recommendations

We recommend that EOUSA:

13. Perform data integrity checks and implement the encryption of data files received to ensure completion and accuracy in accordance with Department policy.

14. Update the VNS system security plan to reflect complete and accurate user identification and authentication security information as required by Department standards.

15. Ensure that a disclaimer notification is developed for the VIS application to notify users when they are about to visit a third-party website through a hyperlink.

16. Modify the VIS application to protect against common web attacks in accordance with the recommendations listed for the specific vulnerabilities in Appendix XI.

17. Terminate unnecessary or vulnerable services identified on the VNS servers.

18. Apply application and server patches in a timely manner.

19. Adequately secure network devices and server configurations in accordance with the recommendations listed for the specific vulnerabilities in Appendix X.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit of the DOJ Victim Notification System (VNS), we considered the Executive Office for U.S. Attorneys' (EOUSA) control structure over the VNS for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurances on its internal control structure as a whole. However, we noted certain matters involving internal controls that we consider reportable matters under the *Government Auditing Standards.*

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operations of the internal control structure that, in our judgment, could adversely affect EOUSA's ability to effectively oversee the VNS. We identified weaknesses in: (1) the management of the VNS, (2) the effectiveness of the VNS, and (3) the information security of the VNS. We discussed these issues in the Findings and Recommendations section of the report. Because we are not expressing an opinion on EOUSA's internal control structure as a whole, this statement is intended for the information and use of EOUSA's management of the VNS.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

In connection with this audit of DOJ's Victim Notification System, as required by *Government Auditing Standards*, we reviewed management processes and records to obtain reasonable assurance about DOJ's compliance with laws and regulations that, if not complied with, in our judgment, could have a material effect on the VNS. Compliance with the laws and regulations applicable to EOUSA's management of the VNS is the responsibility of EOUSA.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations are contained in the relevant portions of the:

- Victim and Witness Protection Act of 1982, Pub. L. No. 97-291;
- Victims of Crime Act of 1984, Pub. L. No. 98-473, the Victims Compensation and Assistance Act, 42 U.S.C. § 10601 (2006), and Services to Victims 42 U.S.C. § 10607 (2007);
- Victims' Rights and Restitution Act of 1990, 42 U.S.C. § 10606 (2004);
- Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. § 14222 (1994);
- Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104 - 132;
- Victim Rights Clarification Act of 1997, 18.U.S.C. § 3510 (1997);
- Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106 – 386; and
- Justice for All Act of 2004, Public Law 108-405.

Our audit did not identify areas where EOUSA was not in compliance with the laws and regulations referred to above. With respect to areas that were not tested, nothing came to our attention that caused us to believe that EOUSA management was not in compliance with the laws and regulations cited above.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to determine if:

(1) EOUSA has effectively managed the VNS, including overseeing the contractors, ensuring the accuracy of data in the system, and planning for the future;

(2) The VNS is an effective tool for victims of crime; and

(3) The VNS was properly secured to prevent unauthorized use, access, and data modification.

Scope and Methodology

To accomplish our audit objectives, we conducted more than 50 interviews with agencies that are directly involved with the VNS, including headquarters officials from EOUSA, the DOJ Criminal Division, the FBI, the BOP, the USPIS, and the OVC. We also spoke with headquarters officials from those agencies that do not directly participate in the VNS, such as the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Drug Enforcement Administration (DEA); the U.S. Marshals Service (USMS); the Administrative Office of the U.S. Courts (AOUSC); the Bureau of Immigration and Customs Enforcement (ICE); and the U.S. Secret Service (USSS) to determine their knowledge of the VNS and whether they had been contacted about participating in the VNS. Additionally, we interviewed the contractor (AT&T Government Solutions) who manages the system, as well as the sub-contractor (Appriss) who manages the Call Center/Help Desk and back-up servers. We also reviewed internal documents, such as planning materials, contracts, manuals, internal directives and policies, and financial reports from EOUSA, the DOJ Criminal Division, the FBI, the BOP, the USPIS, and the OVC. Moreover, we obtained and analyzed empirical data from the VNS and used this information to develop descriptive statistics on the number and types of victims in the system.

We conducted fieldwork in Chicago and Lisle, Illinois; Lexington and Louisville, Kentucky; Kansas City and Leavenworth, Kansas; and Kansas City, Missouri, where we interviewed field personnel. Specifically, at these locations we spoke with senior management and staff who utilized the VNS at the local USAO, BOP, and FBI offices, and reviewed reports and files applicable to our review. In general, the scope of our audit covered the period of FYs 1998 through 2007.

Related to our first objective, we performed a limited review of the services provided by the contractor and sub-contractor – including Call Center operations, discussed the entry of information into the VNS with federal VNS users, reviewed data in the VNS and spoke with federal VNS users to determine if information in the system was accurate, and interviewed non-participating agencies to determine if outreach was performed and if the agencies were interested in participating in the VNS. To determine if the VNS is an effective tool for victims, we designed and deployed two surveys: (1) one to victims who were active in the system, and (2) another to victims who were no longer active in the system.[51] We selected stratified, statistical samples of victims, to which we sent the surveys.[52] We also reviewed other surveys conducted by EOUSA and the BOP, and conducted our own testing of the VNS website through use of a test victim account.

To accomplish our third objective, we utilized a private auditing firm, with experience in conducting IT audits, to perform an information security review of the VNS. Specifically, the OIG engaged Urbach, Kahn, & Werlin, LLP (UKW) to conduct an independent assessment to determine whether VNS information security and privacy policies comply with government standards and established best practices. To identify whether the VNS complied with DOJ and federal privacy and information security policies, UKW performed interviews, on-site observations, and reviews of information security-related documents.

Prior Reviews

The OIG has not performed any prior reviews of DOJ's Victim Notification System. In July 2003, the Government Accountability Office (GAO) reviewed whether EOUSA had institutionalized key information technology (IT) management capabilities that are critical to achieving DOJ's strategic goal of improving the integrity, security, and efficiency of its IT systems. The report identified the VNS as one of EOUSA's systems. The GAO report recommended EOUSA: (1) designate institutionalization of each of the IT management disciplines as priorities, and (2) develop and implement action plans in each of the four IT disciplines to address the weaknesses that were identified in its report. EOUSA agreed with the majority of the GAO's findings and recommendations and stated that it would address most of the recommendations. EOUSA also stated that it has

[51] Copies of both of our surveys can be found in Appendices V and VI.

[52] Due to the technical nature of the work, details of the surveys' complete scope and methodology can be found in Appendices VII and VIII.

made notable progress in institutionalizing the IT management disciplines, particularly information security, and that each was an office priority.

LAWS, REGULATIONS, AND MANDATES ENACTED FOR VICTIMS OF CRIME

Victim and Witness Protection Act of 1982

The VWPA was enacted to: (1) enhance and protect the necessary role of crime victims and witnesses in the criminal justice process, (2) ensure that the federal government does all that is possible within limits of available resources to assist victims and witnesses of crime without infringing on the constitutional rights of defendants, and (3) provide a model for legislation for state and local governments.

Victims of Crime Act of 1984, the Victims Compensation and Assistance Act, and Services to Victims

The Victims of Crime Act of 1984 (VOCA), established the Crime Victims Fund (Fund). The Fund consists of: (1) most fines collected from persons convicted of offenses against the United States; (2) penalty assessments collected under section 3013 of Title 18; (3) proceeds of forfeitures (appearance bonds, bail bonds, and collateral) under section 3146 of Title 18; (4) any money ordered to be paid into the Fund under section 3671 (c)(2) of Title 18; and (5) authorized gifts, bequests, or donations to the Fund from private entities or individuals. The money from this fund was initially to be used for state and local programs for victims of crime. Amended in 1988, the VOCA also legislatively created the Office for Victims of Crime (OVC) within the Office of Justice Programs (OJP). The VOCA was reauthorized and amended in 2005.

In the first session of the 105th Congress, the Fund received a $21 million repayment. Congress authorized these dollars for hiring victim/witness coordinators in the U.S. Attorney's offices; establishing an automated victim information and notification system for federal cases; and collecting, enforcing, and processing restitution orders.

The VOCA also requires responsible officials to identify victims.[53] At the earliest opportunity after the detection of a crime at which it may be done without interfering with an investigation, a responsible official shall: (1) identify the victim or victims of a crime; (2) inform the victims of their right to receive services (described below) on request; and (3) inform each victim of the name, title, and business address and telephone number of the responsible official to whom the victim should address a request for each of the services. Description of services provided under the VOCA are:

(1) A responsible official shall inform a victim: (A) of the place where the victim may receive emergency medical and social services; (B) of any restitution or other relief to which the victim may be entitled under this or any other law and in a manner in which such relief may be obtained; (C) of public and private programs that are available to provide counseling, treatment, and other support to the victim; and (D) of assistance in contacting the persons who are responsible for providing the services and relief.

(2) A responsible official shall arrange for a victim to receive reasonable protection from a suspected offender and persons acting in concert with or at the behest of the suspected offender.

(3) During the investigation and prosecution of a crime, a responsible official shall provide a victim the earliest possible notice of: (A) the status of the investigation of the crime, to the extent it is appropriate to inform the victim and to the extent that it will not interfere with the investigation; (B) the arrest of a suspected offender; (C) the filing of charges against a suspected offender; (D) the scheduling of each court proceeding that the witness is either required to attend or, under section 10606 (b)(4) of this title, is entitled to attend; (E) the release or detention status of an offender or suspected offender; (F) the acceptance of a plea of guilty or nolo contendere or the rendering of a verdict after trial; and (G) the sentence imposed on an offender, including the date on which the offender will be eligible for parole.

[53] The term "victim" means a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime. This includes an institutional entity where there is an authorized representative for the entity. And, in cases where a victim is under 18 years of age, incompetent, incapacitated or deceased, there is another preferred person designated on the victim's behalf (e.g., spouse, legal guardian, parent, a child, a sibling, another family member or another person designated by the court). 42 U.S.C. § 10607 (2007).

(4) During court proceedings, a responsible official shall ensure that a victim is provided a waiting area removed from and out of the sight and hearing of the defendant and defense witnesses.

(5) After trial, a responsible official shall provide a victim the earliest possible notice of: (A) the scheduling of a parole hearing for the offender; (B) the escape, work release, furlough, or any other form of release from custody of the offender; and (C) the death of the offender, if the offender dies while in custody.

(6) At all times, a responsible official shall ensure that any property of a victim that is being held for evidentiary purposes be maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.

(7) The Attorney General or the head of another department or agency that conducts an investigation of a sexual assault shall pay, either directly or by reimbursement of payment by the victim, the cost of a physical examination of the victim, which an investigating officer determines was necessary or useful for evidentiary purposes.

(8) A responsible official shall provide the victim with general information regarding the corrections process, including information about work release, furlough, probation, and eligibility for each.

Victims' Rights and Restitution Act of 1990

The Crime Control Act of 1990 further directed responsible government officials to provide victims with general information regarding the corrections process, including information about work release, furlough, and probation. Title IV of the Victims Rights and Restitution Act of 1990 requires all federal law enforcement agencies to make their best efforts to accord victims of crime with the right to: (1) be treated with fairness and respect for the victim's dignity and privacy; (2) be protected against their accused offenders; (3) be notified of court proceedings; (4) attend public court proceedings related to the offense under certain conditions; (5) confer with the government attorney assigned to the case; (6) receive restitution; and (7) receive information about the conviction, sentencing, imprisonment, and release of the offender. The Act also directs federal law enforcement agency heads to designate the persons required by this Act to identify and provide certain services to the victims of a crime, such as informing victims about where to receive medical care, counseling, and police protection, and about developments during the investigation and prosecution of the crime and

after the trial (such as the arrest of a suspected offender or an escape of a convicted offender). It also directs that a responsible official provide the victim with general information regarding the corrections process, including information about work release, furlough, and probation. This Act was repealed in 2004 and replaced with the Justice for All Act of 2004.

Violent Crime Control and Law Enforcement Act of 1994

The Violent Crime Control and Law Enforcement Act of 1994 mandated that: (1) law should provide for a victim's right of allocation at a sentencing hearing and at any parole hearing if the offender has been convicted of a crime of violence or sexual abuse; (2) such a victim should have an opportunity equivalent to that accorded to the offender's counsel to address the sentencing court or parole board and to present information in relation to that sentence imposed or to the early release of the offender; and (3) if the victim is unable or chooses not to testify at a sentencing or parole hearing, the victim's parents, legal guardian, or family members should have the right to address the court or board. It also established mandatory restitution for victims of four categories of crime: (1) domestic violence, (2) sexual assault, (3) the exploitation and abuse of children, and (4) telemarketing fraud.

Antiterrorism and Effective Death Penalty Act of 1996

The Antiterrorism and Effective Death Penalty Act of 1996 expanded mandatory restitution to virtually all crimes committed in violation of Title 18 of the United States Code.

Victim Rights Clarification Act of 1997

The Victims Rights Clarification Act of 1997 gives victims the right to attend a trial even though they may testify during the sentencing portion of the trial.

The Victims of Trafficking and Violence Protection Act of 2000

The Victims of Trafficking and Violence Protection Act of 2000 protects immigrant victims of domestic violence, human trafficking, and other crimes from deportation in certain cases.

The Justice for All Act of 2004

The 2004 Justice for All Act expanded and recodified the victims' bill of rights and gave victims standing to enforce those rights.[54] The JFAA updated victims' rights to include: (1) the right to be reasonably protected from the accused; (2) the right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused; (3) the right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding; (4) the right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding; (5) the reasonable right to confer with the attorney for the government in the case; (6) the right to full and timely restitution as provided in law; (7) the right to proceedings free from unreasonable delay; and (8) the right to be treated with fairness and with respect for the victim's dignity and privacy.

The JFAA also created the following requirements for government agencies' best efforts to accord victims' rights: (1) government officers and employees of DOJ and other departments and agencies of the United States engaged in the detection, investigation, or prosecution of crime shall make their best efforts to see that crime victims are notified of, and accorded, the rights; (2) the prosecutor shall advise the crime victim that he or she can seek the advice of an attorney with respect to the rights; and (3) notice of release otherwise required pursuant to this chapter shall not be given if such notice may endanger the safety of any person.

The JFAA authorized appropriation funding through VOCA for enhancement of the VNS from 2006-2009.

The Attorney General Guidelines for Victim Witness Assistance (1995, 2000 and 2005)

The purpose of the AG Guidelines was to establish guidelines to be followed by officers and employees of DOJ investigative, prosecutorial, and correctional agencies in the treatment of victims and witnesses to crime.

In the VWPA, Congress instructed the Attorney General to develop and implement guidelines for DOJ consistent with the purposes of the Act. Congress set forth the objectives of the guidelines, which include the

[54] The list of rights, commonly referred to as the "victims' bill of rights" is now codified at 18 U.S.C. § 3771 (2004).

provision of services to victims; notification about protection, services, and major case events; consultation with the government attorney; a separate waiting area at court; the return of property; notification of employers; and training for law enforcement and others. Congress also instructed the Attorney General to assure that all federal law enforcement agencies outside of DOJ adopt guidelines consistent with the purposes of the VWPA.

In conformance with the congressional directive, the Attorney General promulgated the AG Guidelines, which have been revised to incorporate new legislative provisions. In 2000, the AG Guidelines were revised to include the Violent Crime Control and Law Enforcement Act of 1994; the Antiterrorism and Effective Death Penalty Act of 1996; and the Clarification Act of 1997. In 2005, the AG Guidelines were revised to include the Victims of Trafficking and Violence Protection Act of 2000 and the Justice for All Act of 2004.

FUNDING THE VNS

The Victims Compensation and Assistance Act (Pub. L. No. 98-473), as amended through the 1984 Victims of Crime Act (VOCA), 42 U.S.C.§ 10601 (2006), established a monetary account known as the Crime Victims Fund (Fund). It contains money derived not from tax dollars, but from fines and penalties that federal criminal offenders must pay as part of their sentences. The largest source of deposits in the Fund comes from criminal fines.

The VOCA established the Office for Victims of Crime (OVC) within DOJ's Office of Justice Programs (OJP). It authorized the Director of the OVC to administer funding to state and federal agencies for their victim assistance and compensation programs through the Fund.

In 1997, the OVC allocated $8 million to support the development of an automated victim information and notification system for the federal justice system. That same year, $21 million was returned to the Fund and made available to the OVC to improve services to crime victims in the federal criminal justice system. Congress authorized the establishment of an automated victim information and notification system for federal cases through this funding.

The OVC and EOUSA entered into an Inter-Agency Agreement in June 1998 whereby funds were made available through the Fund for the establishment of an automated notification system and to pay for an assessment analysis. EOUSA spearheaded the project, with the assistance from a working group comprised of representatives from the FBI, the OVC, and the BOP.

The VNS working group hired an outside consulting agency to analyze each component's requirements for an automated system, review current available systems that might be expanded to meet the specific needs of the initiative, and develop the system. The analysis was completed January 1999 and the system was deployed in 2001.

The cost of the notification system was estimated to be $8 million and by FY 2000 that amount was transferred from the OVC to EOUSA in reimbursable agreements. Specifically, $559,121 was transferred to EOUSA in FY 1998 for requirement analysis; $193,764 was added to VNS funding for salary, benefit, and travel costs for the VNS Program Manager in FY 1999; and approximately $7.2 million was added for the deployment of the system in FY 2000. The expected outcome of this system was to develop an automated victims' information database and a means to provide

timely victim notification of the current status of offenders in the federal criminal justice system.

The Justice for All Act of 2004 (Pub. L. No. 108-405) authorized appropriations of $2 million for FY 2005 and $5 million in each fiscal year from 2006 through 2009 to the OVC for enhancement of the VNS. Review of the Reimbursable Agreements between the OVC and EOUSA indicate the actual funding approved each year starting in FY 1998, as displayed in the following table.

Reimbursable Agreements between the OVC and EOUSA for the VNS	
Fiscal Year	**Amount**
1998	$559,122
1999	$193,765
2000	$7,199,096
2001	$0
2002	$5,000,000
2003	$5,141,843
2004	$5,141,843
2005	$4,960,000
2006	$5,334,928
2007	$5,000,000
Total	**$38,530,597**

Source: EOUSA Reimbursable Agreements

APPENDIX IV

TYPES OF NOTIFICATIONS

	NOTIFICATION EVENT	DESCRIPTION
FBI/USPIS		
1	Initial (Investigative Agency)	Initial registrant notification from an investigative agency
2	Under Investigation	Case is under investigation
3	Arrest	An anonymous arrest has been made
4	Declination of Prosecution	Declination of prosecution
5	Other (Investigative Agency)	Other notification from an Investigative agency
6	Advice of Victim Rights (Investigative)	Advice of victim rights for an investigative case
7	Investigation Closed	Case not prosecuted
USAO/CRIMINAL DIVISION		
8	Advice of Victim Rights (USAO)	Advice of victim rights for a USAO case
9	Appeal	Appeal
10	Appeal Outcome	The outcome of an appeal by a subject
11	Arraignment	Arraignment hearing
12	Arraignment Canceled	Arraignment hearing canceled
13	Arrest (USAO)	An arrest has been made on a particular subject
14	Bail/Detention Hearing	Bail or detention hearing
15	Bail/Detention Hearing Canceled	Bail or detention hearing canceled
16	CCTV Accepted	Registrant accepted into CCTV program
17	CCTV Initial	Initial CCTV notification
18	CCTV Other	Other CCTV notification
19	CCTV Rejected	Registrant rejected from CCTV program
20	CCTV Scheduled	CCTV event scheduled
21	Change of Plea	The subject has changed his / her plea
22	Change of Plea Canceled	Change of plea canceled
23	Charges Dismissed	Dismissal of charges
24	Charges Filed (includes Victim Rights)	Charges filed against a subject on a docket
25	Competency Hearing	A hearing to determine the competency of the defendant

	NOTIFICATION EVENT	DESCRIPTION
26	Competency Hearing Canceled	Competency hearing canceled
27	Criminal Default Hearing	Collection Hearing 4
28	Criminal Default Hearing Canceled	Collection Hearing 4 canceled
29	Death during Trial	Death during trial
30	Delinquent/Sentencing	Outcome of sentencing for a juvenile subject
31	Directed Verdict	Directed verdict
32	First Appearance	First (or initial) appearance
33	First Appearance Canceled	First appearance canceled
34	Guilty Plea	Guilty plea
35	Hung Jury	The trial has ended due to a hung jury
36	Initial (USAO)	Initial registrant notification from USAO
37	Juvenile Form	Form returned by victim for juvenile subject
38	Mental Treatment Hearing	A hearing for status of defendants found not guilty by reason of insanity
39	Mental Treatment Hearing Canceled	Mental treatment hearing canceled
40	Mistrial	The trial has ended due to a mistrial
41	Oral Argument Appeal Hearing	A hearing to consider an appeal filed in the criminal case.
42	Oral Argument Appeal Hearing Canceled	Oral argument appeal hearing canceled
43	Other Hearing	Other hearing
44	Other (USAO)	Other notification from USAO
45	Other Canceled	Other hearing canceled
46	Plea of Nolo Contendere	Plea of Nolo Contendere
47	Post Trial Hearing	A hearing after plea / verdict before sentencing to cover any issues other than sentencing
48	Post Trial Hearing Canceled	Post trial hearing canceled
49	Preliminary Hearing	Preliminary hearing
50	Preliminary Hearing Canceled	Preliminary hearing canceled
51	Pre-Sentence Hearing	A hearing to cover pre-sentencing issues
52	Pre-Sentence Hearing Canceled	Pre-sentence hearing canceled
53	Pretrial Diversion - Dismissal for	Subject successfully completed pretrial diversion program

	NOTIFICATION EVENT	DESCRIPTION
54	Pretrial Diversion - Enter	Subject entered pretrial diversion program
55	Pretrial Motions Hearing	A hearing to consider pretrial motions
56	Pretrial Motions Hearing Canceled	Pretrial motions hearing canceled
57	Proposed Dismissal of Charges	Charges against a subject have been proposed dismissed
58	Proposed Plea Agreement	Proposed plea agreement for a defendant
59	Release	General release
60	Re-sentencing Hearing	Re-sentencing hearing
61	Re-sentencing Hearing Canceled	Re-sentencing hearing canceled
62	Restitution	A victim has been awarded restitution
63	Restitution Discovery Hearing	Collection Hearing 2
64	Restitution Discovery Hearing Canceled	Collection Hearing 2 canceled
65	Restitution Enforcement Hearing	Collection Hearing 1
66	Restitution Enforcement Hearing Canceled	Collection Hearing 1 canceled
67	Restitution Payment Schedule Hearing	Collection Hearing 3
68	Restitution Payment Schedule Hearing Canceled	Collection Hearing 3 canceled
69	Restitution Re-sentencing Hearing	Collection Hearing 5
70	Restitution Re-sentencing Hearing Canceled	Collection Hearing 5 canceled
71	Revoke/Modify Probation Hearing	A hearing to revoke or modify the conditions of probation.
72	Revoke/Modify Probation Hearing Canceled	Revoke or modify probation hearing canceled
73	Revoke/Modify Supervised Release Hearing	A hearing to revoke or modify supervised release as a result of violations of release.
74	Revoke/Modify Supervised Release Hearing Canceled	Revoke or modify supervised release hearing canceled
75	Rule 20 Transfer Notice	Case is being transferred to another district

APPENDIX IV

	NOTIFICATION EVENT	DESCRIPTION
76	Rule 35 Sentence Reduction Hearing	A hearing to reduce the defendant's sentence
77	Rule 35 Sentence Reduction Hearing Canceled	Rule 35 sentence reduction hearing canceled
78	Sentencing	Sentencing hearing
79	Sentencing Canceled	Sentencing hearing canceled
80	Sentencing Outcome	Outcome of sentencing hearing
81	Status Hearing	A hearing to determine the current status of the case
82	Status Hearing Canceled	Status hearing canceled
83	Subject Detained	A subject has been detained
84	Suppress Evidence/Return Property Hearing	A hearing to suppress evidence or return seized property
85	Suppress Evidence/Return Property Hearing Canceled	Suppress evidence or return seized property hearing canceled
86	Trial (Bench) Verdict (Guilty)	Bench trial verdict (guilty)
87	Trial (Bench) Verdict (Not Guilty)	Bench trial verdict (not guilty)
88	Trial Date	Trial date
89	Trial Date Canceled	Trial date canceled
90	Pretrial Diversion - Unsuccessful	Subject was unsuccessful in the Pretrial Diversion program
91	Verdict (Delinquent)	Delinquent verdict for juvenile subject
92	Verdict (Guilty)	Guilty verdict
93	Verdict (Not Delinquent)	Not delinquent verdict for juvenile subject
94	Verdict (Not Guilty)	Not guilty verdict
95	Verdict Not Guilty Reason of Insanity (Court)	Verdict reason of insanity (court)
96	Verdict Not Guilty Reason of Insanity (Jury)	Verdict reason of insanity (jury)
97	Victim Impact Statement	Request for comments on subject's impact to victim
BOP		
98	Initial Designation	Initial designation
99	Escape while Incarcerated	Escape while incarcerated in a BOP facility
100	Release to Halfway House	Release to halfway house
101	Parole Hearing	Parole hearing
102	Release to Street	Release to street from BOP

APPENDIX IV

	NOTIFICATION EVENT	DESCRIPTION
103	Re-designation	Transferred/re-designated to another BOP location
104	Release on Furlough	Release on furlough
105	Pre-sentenced to Street	Released to street from BOP before release date
106	Death	Death of inmate while in BOP
107	Initial (BOP)	Initial registrant notification from BOP
108	Other (BOP)	Other notification from BOP
109	Apprehension After Escape	Inmate apprehended after escaping
110	Parole Hearing Record Review	Inmate parole hearing record review
111	Sentence Reduction	Inmate sentence reduction
112	Court Dismissed Case	Court dismissed charges on its own initiative
113	Compassionate Release	Inmate considered for compassionate release
114	State Concurrency (Victim)	Inmate sentenced to state prison term
115	State Concurrency (State)	Inmate sentenced to state prison term
116	U.S. Military Clemency Hearing	U.S. military clemency hearing
117	Supervised Release Violator	Subject has violated supervised release
118	Immediate Release to Street	Release inmate to street immediately
119	Conditional Release (Mental Health)	Conditional release (mental health)
ALL		
120	No Longer a Victim	Victim opted-out after federal government determined legal definition of victim not met

APPENDIX V

OFFICE OF THE INSPECTOR GENERAL
OPT-IN SURVEY

GENERAL INFORMATION

The Department of Justice developed the Victim Notification System (VNS) to provide important information to victims. Our records indicate that you are or were a victim of a federal crime (or an alternate contact for a victim) and that you are currently participating in the VNS. Please take a few moments to answer the questions that apply to your situation. Your responses will help improve the VNS.

1. Did you receive an *Initial Notification Letter* from a federal agency informing you about the Victim Notification System? This letter included your registrant identification and pin numbers.
[Check (√) one that applies.]

   ☐ Yes
   ☐ No
   ☐ I do not recall

2. When was the last time you received a notification or when did you last access the VNS website?
[Fill in or check (√) one that applies.]

   ☐ _____
   (month/year)
   ☐ I do not recall.
   ☐ I have not received any notification from the VNS.

3. Please indicate all forms of communication you receive regarding the Victim Notification System: [Check (√) all that apply.]

   ☐ E-mail
   ☐ Fax
   ☐ Letter (U.S. Mail)
   ☐ Pager
   ☐ Telephone
   ☐ TDD (hearing impaired)
   ☐ Website
   ☐ None

4. Which language did you request for your notifications?

☐ English
☐ Spanish
☐ Other
☐ Did not specify language

4a. Did you receive your notifications in the language you requested?

☐ Yes
☐ No

CUSTODY STATUS AND RESTITUTION

The Victims of Crime Act and Justice for All Act include the rights to be reasonably protected from the accused and to full and timely restitution as provided by the law.

5. How important is it for you to know the custody status (incarcerated or not incarcerated) of the defendant(s)/inmate(s) in your case? [Check (√) one that applies.]

☐ Extremely important
☐ Very important
☐ Important
☐ Not important
☐ Not important at all (Go to Question #8.)

6. Are you currently aware of the custody status of the defendant(s)/inmate(s) in your case (out on bail, detained, escaped, died, case dismissed, released, etc.)? [Check (√) one that applies.]

☐ Yes
☐ No

7. Do you know how to find the custody status of the defendant(s)/inmate(s) in your case? [Check (√) one that applies.]

☐ Yes
☐ No (Go to Question #8.)

7a. If yes, have you called any of the following entities regarding custody status of the defendant(s)/inmate(s) in your case? [Check (√) all that apply.]

- ☐ Investigative Agency (FBI/USPIS)
- ☐ U.S. Attorneys Office
- ☐ VNS Call Center
- ☐ Other _____
- ☐ I have not called any of the above entities

7b. How satisfied were you with the assistance you received regarding custody status of the defendant(s)/inmate(s) in your case? [Check (√) one that applies.]

- ☐ Extremely satisfied
- ☐ Very satisfied
- ☐ Satisfied
- ☐ Dissatisfied
- ☐ Very dissatisfied
- ☐ Extremely dissatisfied – if dissatisfied, please explain why in the space below.

8. Are you a victim of a crime that involves restitution? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #10.)

8a. If yes, have you called any of the following entities for assistance regarding restitution?
[Check (√) all that apply.]

- ☐ Investigative Agency (FBI/USPIS)
- ☐ U.S. Attorneys Office
- ☐ VNS Call Center
- ☐ Other _____
- ☐ I have not called any of the above entities.

8b. How satisfied were you with the assistance you received regarding restitution? [Check (√) one that applies.]

☐ Extremely satisfied
☐ Very satisfied
☐ Satisfied
☐ Dissatisfied
☐ Very dissatisfied
☐ Extremely dissatisfied – if dissatisfied, please explain why in the space below.

9. Have you accessed the VNS website for information regarding restitution? [Check (√) one that applies.]

☐ Yes
☐ No
☐ Do Not Recall

9a. If yes, how satisfied were you with the restitution information you received?

☐ Extremely satisfied
☐ Very satisfied
☐ Satisfied
☐ Dissatisfied
☐ Very dissatisfied
☐ Extremely dissatisfied – if dissatisfied, please explain why in the space below.

APPENDIX V

WRITTEN, VERBAL, AND WEBSITE NOTIFICATIONS

The DOJ Victim Notification System is based on a victim's right to reasonable, accurate, and timely notice of any public court or any parole proceeding involving the crime; or of any release or escape of the accused. The following questions relate to the different forms of notification (written, verbal, and website) by which victims in the VNS are notified .

The following questions relate to written notifications via the U.S mail, e-mail, fax, and information posted on the VNS website.

10. How easy is it for you to understand the information in the notifications? [Check (√) one that applies.]

- ☐ Very easy to understand
- ☐ Easy to understand
- ☐ Understandable
- ☐ Difficult to understand
- ☐ Very difficult to understand
- ☐ Extremely difficult to understand

11. Has there been conflicting information in any of the notifications you received? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #12.)

11a. If yes, did you report the conflicting information to the federal agency that sent you the notification(s)? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #12.)

11b. If yes, did the agency resolve the conflict(s)? [Check (√) one that applies.]

- ☐ Yes
- ☐ No

12. Have you ever found incorrect information in any notifications that you have received? [Check (√) one that applies.]

☐ Yes
☐ No (Go to Question #13.)
☐ I do not know (Go to Question #13.)

12a. If yes, did you report the incorrect information to the federal agency that sent you the notification? [Check (√) one that applies.]

☐ Yes
☐ No (Go to Question #13.)

12b. If yes, did the agency correct the incorrect information? [Check (√) one that applies.]

☐ Yes
☐ No

13. In your opinion, do you agree or disagree that you have been notified of *all* events (such as public court proceedings) involving your case? [Check (√) one that applies.]

☐ Strongly agree
☐ Agree
☐ Neutral
☐ Disagree
☐ Strongly disagree
☐ I do not know.

14. Do you agree or disagree that you received *timely* notices well before the events? [Check (√) one that applies.]

☐ Strongly agree (Notices were received well before the events.) (Go to Question #15.)
☐ Agree (Go to Question #15.)
☐ Neutral (Go to Question #15.)
☐ Disagree
☐ Strongly disagree (Notices were *not* received well before the events.)

14a. If notices were not *timely*, how often did you receive late notifications? [Check (√) one that applies.]

- ☐ 1-3 times
- ☐ 4-6 times
- ☐ 7-9 times
- ☐ 10 times or more

14b. If notices were not *timely*, did you ever miss an event you wanted to attend because of a late notification? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #15.)

14c. If yes, how many events did you miss? [Check (√) one that applies.]

- ☐ 1-3 events
- ☐ 4-6 events
- ☐ 7-9 events
- ☐ 10 events or more

15. Did you participate in any event (for example, attend, speak, or submit a victim impact statement) after receiving a notification? [Check (√) one that applies]

- ☐ Yes
- ☐ No
- ☐ Not applicable

16. Were you ever not able to attend an event because the notification was unclear or contained conflicting information? [Check (√) one that applies]

- ☐ Yes
- ☐ No
- ☐ Not applicable

17. Overall, how useful was the information provided to you in the notification(s)? [Check (√) one that applies.]

- ☐ Very useful
- ☐ Useful
- ☐ Neutral
- ☐ Not useful
- ☐ Not at all useful

The following questions pertain to the VNS Internet Website.

18. Have you ever accessed the VNS website to review your case information? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #30.)

19. How easy or hard was the process to set up your VNS website account? [Check (√) one that applies.]

- ☐ Very easy
- ☐ Somewhat easy
- ☐ Neither hard nor easy
- ☐ Somewhat hard
- ☐ Very hard

20. How easy or hard is it to navigate or find information within the VNS website? [Check (√) one that applies.]

- ☐ Very easy
- ☐ Somewhat easy
- ☐ Neither hard nor easy
- ☐ Somewhat hard
- ☐ Very hard

21. How often have you accessed the VNS website for information? [Check (√) one that applies.]

- ☐ Every day
- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly
- ☐ Annually
- ☐ I have not accessed the website since I set up my account.

22. How easy was it for you to understand the information on the website? [Check (√) one that applies.]

- ☐ Very easy to understand
- ☐ Easy to understand
- ☐ Neither easy or difficult to understand
- ☐ Difficult to understand
- ☐ Very difficult to understand

23. Did you find all the information you wanted on the website? [Check (√) one that applies.]

- ☐ Found all information
- ☐ Found almost all information
- ☐ Found some information
- ☐ Found little information
- ☐ Did not find information

24. Was there conflicting information on the website? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #25.)

24a. If yes, did you report the conflicting information to any of the following entities? [Check (√) all that apply.]

- ☐ Investigative agency
- ☐ U.S. Attorneys Office
- ☐ VNS Call Center
- ☐ Other

☐ I did not report the conflicting information.
(Go to Question #25.)

24b. Were information conflicts resolved? [Check (√) one that applies.]

☐ Yes
☐ No

25. Have you ever come across incorrect information in the website? [Check (√) one that applies.]

☐ Yes
☐ No (Go to Question #26.)
☐ I do not know (Go to Question #26.)

25a. If yes, did you report the incorrect information to any of the following entities? [Check (√) all that apply.]

☐ Investigative agency
☐ U.S. Attorneys Office
☐ VNS Call Center
☐ Other
☐ I did not report the incorrect information.

25b. Was the incorrect information corrected? [Check (√) one that applies.]

☐ Yes
☐ No

26. In your opinion, do you agree or disagree that notice of event(s) was posted on the VNS website in a timely manner? [Check (√) one that applies.]

☐ Strongly agree (Go to Question #27.)
☐ Agree (Go to Question #27.)
☐ Neutral (Go to Question #27.)
☐ Disagree
☐ Strongly disagree

26a. If you disagree, did you miss an event because the information was posted too late?

[Check (√) one that applies.]

☐ Yes
☐ No

26b. How often have you noticed late posting(s) on the website? [Check (√) one that applies.]

☐ 1-3 times
☐ 4-6 times
☐ 7-9 times
☐ 10 times or more

27. Have you participated in any event (for example, attend, speak, or submit a victim impact statement) after reviewing VNS website information? [Check (√) one that applies]

☐ Yes
☐ No

28. Overall, how useful is the information provided to you on the website?
[Check (√) one that applies.]

☐ Very useful
☐ Useful
☐ Neutral
☐ Not useful
☐ Not at all useful

29. If any, what information would you like to see added to the website?
(Please print your answer below.)

CALL CENTER – AUTOMATED INFORMATION AND LIVE ASSISTANCE

The following questions relate to the VNS Call Center, which provides victims with automated information and/or live assistance with their case, or live assistance with the VNS website.

30. Have you called the toll-free number to get Call Center assistance? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #46.)
- ☐ I do not recall (Go to Question #46.)

30a. If yes, what type of assistance did you receive from the Call Center? [Check (√) all that apply.]

- ☐ Automated Assistance
- ☐ Live Assistance
- ☐ Both

31. Have you ever contacted the Call Center and hung up for any of the following reason(s)? [Check (√) all that apply.]

- ☐ It took too long to get help.
- ☐ There were too many instructions to follow.
- ☐ The automated call system was too difficult to use.
- ☐ Other (please describe)

Please answer Questions #32-37 only if you have used the Call Center's automated system for case information; otherwise go to Question #38.

32. How often have you used the *automated* system? [Check (√) one that applies.]

- ☐ Often
- ☐ Sometimes
- ☐ Rarely
- ☐ Never (Go to Question #38.)

33. How would you rate the *automated* system availability when you called? [Check (√) one that applies.]

- ☐ Always available
- ☐ Often available
- ☐ Sometimes available
- ☐ Rarely available
- ☐ Never available

34. How easy is it to access information through the *automated* system? [Check (√) one that applies.]

- ☐ Very easy
- ☐ Easy
- ☐ Somewhat easy
- ☐ Not easy
- ☐ Not easy at all

35. Is the information easy to hear on the *automated* system? [Check (√) one that applies.]

- ☐ Yes
- ☐ No

36. Did you receive the information you wanted from the *automated* system? [Check (√) one that applies.]

- ☐ Always received the information
- ☐ Often received the information
- ☐ Sometimes received the information
- ☐ Rarely received the information
- ☐ Never received the information

37. What additional information would you like made available from the Call Center's *automated system for case information*? Please print your answer below.

Answer Questions #38-41 only if you used live assistance for case information; otherwise go to Question #42.

38. How often have you used *live assistance* from the Call Center? [Check (√) one that applies.]

- ☐ Often
- ☐ Sometimes
- ☐ Rarely
- ☐ Never (Go to Question #42.)

39. How would you rate the *live assistance* availability when you called? [Check (√) one that applies.]

- ☐ Always available
- ☐ Often available
- ☐ Sometimes available
- ☐ Rarely available
- ☐ Never available

40. Did you receive the information you wanted? [Check (√) one that applies.]

- ☐ Always received the information
- ☐ Often received the information
- ☐ Sometimes received the information
- ☐ Rarely received the information
- ☐ Never received the information

41. What additional information would you like made available from the Call Center's *live assistance for case information*? Please print your answer below.

Answer Questions #42-45 only if you used the Call Center for VNS website assistance; otherwise go to Question #46.

42. Have you ever contacted the Call Center for *VNS website assistance*? [Check (√) one that applies.]

- ☐ Yes
- ☐ No (Go to Question #45.)

43. For which of the following did you need *VNS website assistance*? [Check (√) all that apply.]

- ☐ Victim Identification Number (VIN)
- ☐ Personal Identification Number (PIN)
- ☐ VNS website access
- ☐ Other VNS website questions (Please print your answer below.)

44. Did you receive the information about the VNS website you wanted from the Call Center *live assistance*? [Check (√) one that applies.]

- ☐ Always received the information
- ☐ Often received the information
- ☐ Sometimes received the information
- ☐ Rarely received the information
- ☐ Never received the information

45. What additional information would you like made available from the Call Center *for VNS website assistance*?
Please print your answer below.

YOUR OPINION COUNTS

Your opinion is very important to help improve the Victim Notification System. Please answer the following questions about your experiences with the services and information provided by the VNS. Please print your answers in the space provided below each question.

46. What are the most beneficial services provided by the VNS?

47. What improvements would you like to see made to the VNS?

48. What additional information in the VNS would be useful to you?

Thank you for taking the time to complete the survey. Your participation is greatly appreciated and will help to improve the Department of Justice Victim Notification System.

OFFICE OF THE INSPECTOR GENERAL
OPT-OUT SURVEY

The U.S. Department of Justice developed the Victim Notification System (VNS) to provide important information to victims. Our records indicate that you are or were a victim of a federal crime (or an alternate contact for a victim), but that you are currently ***not*** *receiving notifications from the VNS. Please take a moment to answer the questions that apply to your situation.*

1. Did you receive an *Initial Notification Letter* from a federal agency informing you about the Victim Notification System that included your registrant identification number and pin number?
[Check (√) one that applies.]

☐ Yes
☐ No
☐ Do not recall

2. Did *you* choose not to receive notification from the Victim Notification System?
[Check (√) one that applies.]

☐ Yes
☐ No (Go to question #3a.)
☐ Do not recall (Go to Question #3a.)

2a. If yes, what was your reason for choosing not to receive notification from the Victim Notification System?

☐ Please print your answer below.

☐ I do not recall the reason given.

3. If it was *not your choice* to stop receiving notification, were you informed by a federal agency that you would no longer receive notification? [Check (√) one that applies.]

☐ Yes
☐ No (Go to question #4.)

3a. If yes, what was the reason given? [Check (√) one that applies.]

☐ Please print your answer below.

☐ I do not recall the reason given. (Go to question #4.)

3b. Was the reason given by the federal government agency to your satisfaction?

☐ I was satisfied.

☐ I was dissatisfied. (Please print your explanation below.)

4. Do you have any additional comments about the Victim Notification System? [Please print your comments below.]

Thank you for taking the time to complete the survey. Your participation is greatly appreciated and will help our review of the Victim Notification System.

APPENDIX VII

OPT-IN SURVEY
SCOPE, METHODOLOGY, AND RESPONSE REVIEW

This appendix describes the approach employed to extract the universe of victims to whom notifications were generated by the VNS during the scope of our review. From this universe, a sample of registrant identification numbers was selected and a questionnaire was sent to the sampled victims. Accordingly, the descriptions of the sample selection process and the survey response review are included in this appendix. Our objective was to determine whether the VNS served its intended purpose and satisfied victims' expectations.

Scope

The scope of our universe consisted of opt-in victims with approved notification information between October 1, 2004, and September 30, 2006. "Opt-in" is the status of a registered victim or contact allowing them to receive notifications and access the VNS phone line and Internet web page.

Methodology

To determine the number of victims registered in the VNS, we requested specific data fields contained in the VNS database between October 1, 2004, and September 30, 2006. We obtained the data to select a sample of victims for our survey deployment.

The VNS creates a unique registrant identification number (Registrant ID) to identify a victim. The Registrant ID data field was used as the anchor data field in the universe extraction process. We requested data for each notification phase (investigative, prosecution, and incarceration) using the Registrant ID as the primary key for opt-in victims. We requested case information, such as the investigative case number, notification event, USAO agency name, USMS inmate number, custody status; and victim information, such as city, state, and country.

Data Organization and Sample Selection

We identified records associated to the opt-in victims and requested the databases from EOUSA. We constructed the opt-in victim universe from the received data download. We uploaded the databases to summarize the data in order to compile the information and link tables to create a universe from which we could select the sample. There were a total of 621,276 registrant IDs we identified that were at least in 1 of the 3 phases during the

scope of our audit. We then removed 4,000 registrant IDs that had previously been surveyed by EOUSA to arrive at our final universe of 618,201 unique sample units. We also created a sub-set of 52,166 registrant IDs from the universe using the incarceration phase's "Notification Event Types" field with events that were related to the release of inmates.

We separated the universe into two categories for U.S. and non-U.S. Registrant IDs using the victim information fields, state, and country. We then stratified the universe of unique Registrant IDs and the incarceration phase release-related events sub-set. We then created nine strata through various grouping of the three phases and the incarceration release-related events using the U.S. Registrant IDs to group them. The tenth stratum included the Registrant IDs with non-U.S. addresses and those with no address information identified. The sample selection process included the sample sizes for each of the 10 strata that were statistically calculated. The total population size was 618,203 Registrant IDs, and the sample size was 2,783.

Survey Response Review

We received a total of 691 surveys mailed back to us by the recipients. We found that some respondents completed the survey, answered only some of the questions, or included a comment without completing the survey. As a result, we reviewed the data to eliminate surveys that did not contain useful information. Upon closer review of the data, we found records of surveys that did not have responses to all the questions in the survey. We identified and excluded those records with non-responses and arrived at a data set of 531 records. We used the data in these 531 records for analysis using the SPSS software package.

Conclusion

Of the total 618,201 unique VNS Registrant ID numbers opted into the system from October 1, 2004, through September 30, 2006, which were suitable for our survey deployment, our sample size was 2,783. We received a total of 691 surveys, of which 531 were considered to have useful responses.

APPENDIX VIII

OPT-OUT SURVEY SCOPE AND METHODOLOGY

The following methodology was employed for data analysis and used to obtain a functional universe for sample selection purposes. The techniques in this analysis include, but were not limited to, exploratory analysis, comparative analysis, and descriptive analysis. We describe the results of the analysis at different phases, reasons for the analysis, and the sample methodology.

In the database of 347,716 opted-out records, there were a total of 71,179 unique VNS Registrant IDs. In order to understand the reasons for opt out, we examined the data and we found four different types of data values and blanks in the field "OPT-OUT REASON" to include invalid address, user choice, contact choice, no longer a victim, and blank fields.

We excluded the 52,029 VNS IDs that were associated with "Invalid Address" and 6,025 records that had no information in both the city and state columns of the database. The final universe of opt-out victims contained 13,125 records (opt-out victims) and only included records that had enough information for sample selection purposes.

In order to obtain a better response rate and useful responses to the questions, we used a stratified sampling plan. The universe of 13,125 unique Registrant IDs was stratified considering the combination of the number of notifications and the values in the "OPT-OUT REASON" field for a total of 489 sample Registrant IDs selected.

Opt-out Survey Response Analysis

There were 58 respondents who responded to the opt-out survey. There were 14 respondents who did not respond to all or most of the questions in the survey. The responses from these 14 respondents were excluded from further analysis. A frequency table of the remaining 44 responses was saved and used for logical tests analyses.

APPENDIX IX

OPT-IN SURVEY QUESTION 41

What additional information would you like made available from the Call Center's live assistance for case information?

No.	Comment
1.	Called once.
2.	Someone who can translate in Navajo- Navajo legal terminology.
3.	Information about restitution.
4.	Plain and simply how to access live assistance. Couldn't figure out how to get live assistance.
5.	Would like phone interview and additional space.
6.	Respond right away if anybody call in emergency case.
7.	The Call Center is hindered by minimal information details that are not readily available.
8.	Survey person discuss what VNS was about.
9.	Don't Know.
10.	Why was information sent to me. I only called to get an explanation of how my name was selected.
11.	Status of restitution- where' my money and when will I get it.
12.	N/A
13.	I am not qualified to answer this.
14.	Is my case or status needed?
15.	Is the criminal in prison? Can we expect restitution of our stolen money?
16.	How to log into my online account. Someone was supposed to send me new info in the mail. I've now been waiting almost one year for it!
17.	XXXXX XXXXX was on vacation.
18.	None

APPENDIX IX

No.	Comment
19.	More detailed information and awareness of the operators. They were uneducated to fully answer my questions.
20.	None
21.	I would like to know more information on how my case is going. I have heard nothing since April, 2006.
22.	Update on the investigation!
23.	Please have me informed what's going on.
24.	I made the initial call in response to a bomb threat. I do not know any information after the initial report.
25.	Actual Assistance
26.	Time frame on our money.
27.	Updated, current info in custody??
28.	Want system to work.
29.	Can't think of anything.

APPENDIX X

THE VICTIM NOTIFICATION SYSTEM'S VULNERABILITY ASSESSMENT RESULTS

[SENSITIVE INFORMATION REDACTED]

APPENDIX XI

THE VICTIM INTERNET SYSTEM'S WEB APPLICATION TESTING RESULTS

[SENSITIVE INFORMATION REDACTED]

APPENDIX XII

EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS RESPONSE

U.S. Department of Justice

Executive Office for United States Attorneys

Office of Legal Programs and Policy

Suite 7600, Bicentennial Building
600 E Street, NW
Washington, D.C. 20530-0001

(202) 616-6444
FAX (202) 616-6647

January 17, 2008

MEMORANDUM

TO: Raymond J. Beaudet
Assistant Inspector General for Audit
Office of the Inspector General

/s/
FROM: Kenneth E. Melson
Director

SUBJECT: Response to OIG Report on the Department's Victim Notification System

Thank you for the opportunity to review the Department of Justice, Office of the Inspector General's (OIG) draft audit report entitled, "The Department of Justice's Victim Notification System." The Executive Office for United States Attorneys (EOUSA) is proud of what it has accomplished with the Victim Notification System (VNS) since its implementation in January 2002. Since that time, 31,891,296 notification events have been provided to over one million victims of federal crimes. The VNS is the most robust system in the country for providing notification to victims of crime, far surpassing any other system in its complexity and the number of notifications sent. It also is the only system which we are aware of that by default opts-in all victims of crimes. Without the system, the United States Attorneys' Offices (USAO) would not be capable of meeting the requirements of the Crime Victims Rights Act to provide victims with notification of all public court proceedings. EOUSA concurs with most of the

recommendations resulting from this review and provides its response below.

Providing notifications to victims requires the cooperation of many organizations beyond EOUSA and we will work with the USAOs, other Department components, and the other government agencies to resolve and implement solutions to the OIG's findings. EOUSA expects the full cooperation of all the parties mentioned in working to continue to improve our ability to provide notifications of public court proceedings to victims of crime and will take all appropriate steps to help achieve compliance with OIG's recommendations.

VNS provides notifications worldwide to victims of every background and experience, regarding an immense array of crimes and types of proceedings. It is necessarily broad and simple in its delivery. Its role is not to provide victims with all information they may want, or to inform victims about the system itself. That role is best handled by individuals who know the facts of the case and can thoroughly explain the situation to a victim. The role of VNS is to assist the Department with its provision of statutorily-mandated victim notifications. EOUSA will continue to seek to improve VNS to ensure that notifications are accurate and timely; however, VNS cannot replace the human interaction by USAO personnel with victims to provide them with additional information concerning their cases.

Documentation detailing EOUSA's efforts to implement the action plan will be provided to the OIG until all corrective actions are taken.

ACTION PLAN

Recommendation 1: **Develop a written plan to: (1) archive VNS data, which should include a schedule for the initial archiving, parameters for subsequent archiving, and the criteria it will utilize to determine the records ready for archiving; or (2) acquire new equipment that will resolve the capacity issue.**

Response to Recommendation 1: Regarding the archiving of data, the OIG found ". . . because data in the VNS has never been archived, storage space on the VNS server has been filled to almost 80 percent of its capacity, affecting both data access speed and performance of the System." Archival of data was included as a contract requirement in order to lessen the impact on system performance. However, EOUSA would note that despite the decline in performance resulting from the capacity issues, the System continued to operate within the

parameters of the contract as evidenced by the monthly performance reports.

During the period covered by the OIG report new equipment was acquired by EOUSA and the installation of that equipment was completed on October 20, 2007. Funding for this equipment was provided in part from the annual OVC grant for VNS ($284,640) and from funds provided by EOUSA ($116,960). The replacement of the old equipment has alleviated the storage space issues for the projected life span of the new equipment and negates the necessity for archiving data. The next VNS contract has been tasked with addressing the issue of data archival in light of the decreasing cost of on-line data storage and the significant technology advances in this area.

Recommendation 2: **Ensure that it is utilizing the newer version of the Tracker software, called Front Range, to allow for a more user-friendly data extraction and reporting function. Further, ensure that Front Range's feature that automatically e-mails the caller upon the closing of a ticket has been enabled and is being utilized to the fullest extent.**

Response to Recommendation 2: As part of the Call Center/Help Desk procedure contacts by victims and government users of the System with the contractor staff are logged and notes of the substance of the contact are maintained. The software used by the contractor for this purpose was Tracker. As noted in the Report on page 13, Tracker was replaced with Front Range on July 5, 2007.

EOUSA does plan to implement the email feature available within Front Range to survey individuals upon the closing of a “ticket” regarding customer satisfaction with the Help Desk. This feature is expected to be implemented in a future release to VNS.

Recommendation 3: **Develop a universal interface for federal investigative agencies to upload data directly to the VNS.**

Response to Recommendation 3: EOUSA has considered the universal interface one of several priorities since we conceived the idea almost three years ago. However, the enactment of the CVRA in 2004 has forced EOUSA to adopt many changes in VNS to accommodate that new law. As noted in the OIG report, funding for VNS actually declined since FY 2004. However, EOUSA accomplished the required changes to implement the CVRA within the declining allocation provided by OVC. Absent those demands on the VNS budget, the

universal interface would likely have been implemented. EOUSA does plan to proceed with the universal interface when adequate funds are made available by OVC.

Recommendation 4: Work with the AOUSC to develop the hardware to connect the VNS and the AOUSC, develop a plan to connect individual federal court districts to the VNS using this interface, and endeavor to ensure that all federal districts are connected to the VNS.

Response to Recommendation 4: EOUSA and AOUSC have agreed to develop the ability to connect individual district courts to VNS. That technical development is underway and the projected completion date is late March 2008. Approximately 94 percent of this project was funded by EOUSA; a minimal amount was funded from the OVC annual grant to EOUSA for VNS. (Total expenditure $726,078, OVC funded $46,038.)

As part of the project with AOUSC, EOUSA intends to develop a plan to promote the connection of the individual district Courts to VNS. We believe this plan will ultimately result in the majority of U.S. District Courts participating in the VNS. However, absent Congressional action, the Department of Justice as part of the Executive Branch of the government will not be able to "ensure" the Courts, as part of the Judicial Branch, connect to VNS.

It must be noted that while EOUSA was able to provide funding for VNS this one fiscal year, we will not be able to continue to supplement funding for VNS in the future and must rely on sufficient funds being provided by OVC to continue with the operation, maintenance and enhancements for this System.

Recommendation 5: **Work with VNS-participating agencies to develop and implement procedures for federal VNS users to ensure that victims' contact information is current and updated.**

Response to Recommendation 5: EOUSA agrees that it is essential that VNS contain current and accurate victim-contact information so that victims receive timely notification of court events. EOUSA also notes that frequently, it is difficult to obtain up-to-date victim contact information during the course of a criminal investigation. For example, in large-victim cases, often the only source of victim contact information is from a defendant's files, and this information can be

incomplete or inaccurate. In addition, victims often will move without informing investigators of their new addresses. In spite of these inherent difficulties, EOUSA will work with VNS-participating agencies to develop and implement additional procedures to ensure that victim contact information is as up-to-date and accurate as possible.

Recommendation 6: **Develop long-range plans for the VNS and its management that include: (1) future software and hardware upgrades, (2) replacement of outdated equipment, (3) expansion of VNS server storage capacity, (4) a projection of enhancements needed to account for the future needs of government and victim users, and (5) a formal succession plan for VNS project management.**

Response to Recommendation 6: (1) Future hardware and software upgrades are currently being addressed by the next VNS contract which is scheduled for award in 2008. That agreement will require the contractor to provide a plan for periodic replacement of VNS hardware and/or software; (2) the "outdated" equipment referred to in the Report was replaced on October 20, 2007; (3) Server storage capacity was resolved with the October 20, 2007 equipment replacement. Future storage issues will be part of the contract life cycle plans incorporated in the next VNS contract (see Response to Recommendation #1) ; (4) Regarding a plan for future enhancements, in early September 2007, EOUSA held a conference for USAO victim/witness staff members at the National Advocacy Center in Columbia, South Carolina. During that conference approximately 67 staff members representing offices from across the country attended a session dedicated to soliciting ideas for improving VNS and long range needs for users and victims. Those ideas will be used in conjunction with the next VNS contract to plan for the future. The new contract will contain provisions for the contractor to evaluate the current technology and to provide proposals for improvements to the System. However, any such long range plans for future needs are subject to sufficient funds, beyond the static allotment which has been furnished to EOUSA for this program since 2002, being made available from OVC; (5) EOUSA is responsible for maintaining several of the Department's largest systems including LIONS, CDCS, and USA-5. Program managers have changed a number of times for these systems and others, so EOUSA does not believe there is reason for concern that there is no written succession plan for the program manager of VNS; however, EOUSA will provide the OIG with a written plan in the near future.

Recommendation 7: Work with VNS-participating agencies to develop and implement a nationwide procedure for addressing undeliverable correspondence and e-mail.

Response to Recommendation 7: Regarding undeliverable email notices, the use of email as a notification method has increased significantly since FY05 due to an engineering change implemented in early FY06. (Successful emails: FY05 - 34,358; FY06 - 598,073; FY07 868,857. Successful means VNS generated and transmitted the email notice.) EOUSA has recognized the need to address the undeliverable email issues, however, the need to devote the limited amount of VNS funding to CVRA related issues has impacted our ability to resolve this matter. The new VNS contract will require a technical solution to this issue; however the technical change cannot be made until sufficient funding is made available.

Regarding undeliverable correspondence, EOUSA does encourage USAOs to make their best efforts to follow up on returned mail to obtain more accurate addresses. Further, it must be acknowledged that it is the responsibility of investigative agencies to ensure that accurate addresses are initially entered into VNS. However, recognizing the importance of ensuring that victims receive notifications, EOUSA will work with other agencies to develop a nationwide policy regarding returned mail.

Recommendation 8: Improve the Call Center automated assistance to allow callers to reach an operator at any point during a call.

Response to Recommendation 8: The current Call Center process, which only allows access to the Help Desk by victims once the ID/PIN is correctly entered, was engineered to provide some authentication for the Help Desk to assist in protecting the victim's personal information in the System. However, we agree the System should permit a caller to reach an operator at any point after the user ID/PIN has been authenticated. An engineering change to allow this access will be considered for a future release to VNS.

Recommendation 9: **Follow up with the sub-contractor at the VNS Call Center to fulfill its requirement to have a Spanish-speaking operator available during all hours of operation.**

Response to Recommendation 9: Section C.5.10(b)(4) of the VNS contract requires: "The victim must also have the option of speaking

directly with a Call Center operator (during Call Center hours of operation, see Section C.6) to obtain case information in either English or Spanish." According to the contractor, about one operator call per month requires a fluent Spanish speaking operator. The VNS Project Manager has discussed the requirement with the VNS contractor. Currently, the Call Center has one fluent Spanish speaker and the remaining staff has some Spanish speaking capability. The contractor is aware of the requirement and is taking steps to recruit Spanish speakers.

In the interim, we have devised a plan which will make use of a department within Appriss which provides Spanish translations. If a Spanish speaker is not available at the Call Center, the Call Center will contact by telephone the Appriss translation department (located in the same building as the VNS Call Center), establish a 3-way call and have the Appriss division provide the translation for the Help Desk. This is intended as temporary solution until such time as the Call Center can hire operators fluent in Spanish.

Recommendation 10: **Work with the USMS to ensure that the accurate custody status of defendants is available to victims utilizing VNS services.**

Response to Recommendation 10: In September 2007, EOUSA funded the cost of the engineering changes which will allow VNS to accept custody status data directly from the USMS. EOUSA has been in contact with USMS regarding this interface between the two systems, and plans to have VNS ready to accept data from USMS by March 2008. Once implemented, the data from USMS will provide VNS and victims with the current custody status of the defendant while their case is being litigated.

Recommendation 11: **Ensure that information regarding restitution is consistent throughout the VIS so that it is clear to victims whether restitution information is available to them.**

Response to Recommendation 11: EOUSA will undertake additional review of VIS regarding the consistency of the information provided regarding the availability of restitution.

Recommendation 12: **Work with VNS-participating agencies to develop a requirement for federal VNS users to record a reason for opting a victim out of the VNS.**

Response to Recommendation 12: EOUSA will request an engineering change to VNS which will require users to select one of the opt-out reasons when electing to stop notifications from being provided to a registered victim. This change will need to be carried over to various screens and reports in VNS involving the opt-out function. When sufficient funding is made available this change will be implemented.

Recommendation 13: Perform data integrity checks and implement the encryption of data files received to ensure completion and accuracy in accordance with Department policy.

Response to Recommendation 13: The EOUSA notes that all VNS data files are validated for format as part of the VNS import process; any incomplete or malformed files are rejected, thereby reducing the risk to system integrity and availability. Partial session encryption, rather than complete session encryption, is utilized for data transfers from the FBI and BOP; thereby providing partial rather than complete assurance of data integrity. The EOUSA VNS Program Management office is currently testing complete session encryption with the FBI, BOP, and the Justice Management Division (Rockville Data Center).

Recommendation 14: Update the VNS system security plan to reflect complete and accurate user identification and authentication security information as required by Department standards.

Response to Recommendation 14: The EOUSA has updated the System Security Plan as appropriate, including revision of user identification and authentication implementation.

Recommendation 15: Ensure that a disclaimer notification is developed for the VIS application to notify users when they are about to visit a third party website through a hyperlink.

Response to Recommendation 15: The VNS Program Management office will implement a disclaimer statement for VIS.

Recommendation 16: Modify the VIS application to protect against common web attacks in accordance with the recommendations listed for the specific vulnerabilities in Appendix XI.

Response to Recommendation 16: The EOUSA will assess VIS application with a leading commercial web application vulnerability assessment utility and implement corrective actions as appropriate. The EOUSA will explicitly test for the vulnerabilities listed in Appendix XI.

Recommendation 17: Terminate unnecessary or vulnerable services identified on the VNS servers.

Response to Recommendation 17: The EOUSA has completed actions to terminate unnecessary services on the VNS servers.

Recommendation 18: Apply application and server patches in a timely manner.

Response to Recommendation 18: The EOUSA Enterprise Vulnerability Management Program (EVMP) scans and assesses VNS networks and systems for vulnerabilities on a regular periodic basis (each month) and also on an irregular ad hoc basis. Application and server patches are analyzed, risks weighed, and finally resolved to either be corrected or accepted as risk. Due to technical and business considerations, not all patches are applied. In accordance with the DOJ IT Security Program Management Plan, the EOUSA will continue to resolve vulnerabilities in a timely manner. Patches selected for implementation will continue to be applied in accordance with documented VNS configuration management processes.

Recommendation 19: Adequately secure network devices and server configurations in accordance with the recommendations listed for the specific vulnerabilities in Appendix X.

Response to Recommendation 19: The EOUSA continues to assess VNS infrastructure on a regular periodic basis with the DOJ standard assessment utility in accordance with the DOJ IT Security Program Plan. Several vulnerabilities listed in Appendix X have been corrected. Others have been confirmed as false positives. The EOUSA will continuously monitor and assess VNS for vulnerabilities and implement corrective actions as appropriate to maintain an acceptable level of risk.

Thank you again for the opportunity to provide comments to the Report.

APPENDIX XIII

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

In its response to our draft audit report, EOUSA concurred with our recommendations. This appendix provides our analyses of EOUSA's responses, including the actions needed to close each recommendation.

Status of Recommendations

1. **Resolved.** In its response to our draft report recommendation to develop a written plan for archiving VNS data or acquiring new equipment to resolve the capacity issue, EOUSA stated that it installed new equipment on October 20, 2007. EOUSA stated that replacing the old equipment has alleviated storage space issues for the projected lifespan of the new equipment. EOUSA further stated that it would address data archiving in the next VNS contract.

   To close this recommendation, please provide us with a copy of the next VNS contract, including information regarding the archiving of VNS data.

2. **Resolved.** In response to our recommendation to ensure that it utilizes the newer version of Tracker software for Call Center/Help Desk functions, EOUSA stated that Tracker was replaced with Front Range on July 5, 2007. EOUSA further stated that in a future release to the VNS, it plans to implement the Front Range e-mail function that surveys individuals upon the closing of a "ticket" regarding customer satisfaction with the Help Desk.

   To close this recommendation, please provide evidence that EOUSA has replaced Tracker with Front Range. Additionally, please provide evidence that EOUSA has implemented the Front Range feature for surveying individuals upon closing of a "ticket."

3. **Resolved.** EOUSA is in agreement with our recommendation to develop a universal interface for federal investigative agencies to upload data directly to the VNS. EOUSA stated that it plans to proceed with the universal interface when funding is made available by the OVC.

To close this recommendation, please provide us with evidence that the universal interface has been developed and is being utilized by federal investigative agencies to upload data directly to the VNS.

4. **Resolved.** In its response to the draft report, EOUSA advised that it and the Administrative Office of the U.S. Courts (AOUSC) have agreed to develop the ability to connect individual district courts to the VNS. Further, EOUSA stated that development is underway and the project is expected to be completed in late March 2008. However, EOUSA noted that it cannot ensure that all district courts are connected because the Courts, as part of the Judicial Branch, are not part of DOJ.

   To close this recommendation, please provide us, when available, evidence that the technical development of an EOUSA/AOUSC interface is complete. Further, please provide us, when developed, with a copy of the plan to promote the connection of the individual district courts to the VNS. Finally, once the plans are complete, please provide us with evidence of individual district courts that agree to be connected to the VNS.

5. **Resolved.** In its response to our recommendation to work with VNS-participating agencies to develop and implement procedures for federal VNS users to ensure that victims' contact information is current and updated, EOUSA agreed that it is essential that the VNS contain current and accurate victim-contact information. According to EOUSA, though, it will work with VNS-participating agencies to develop and implement additional procedures to ensure that victim contact information is as up-to-date and accurate as possible.

   To close this recommendation, please provide us with evidence of your efforts to work with VNS-participating agencies to develop and implement additional procedures to ensure that victim contact information is as up-to-date and accurate as possible.

6. **Resolved.** EOUSA provided information, by specific area, in response to our recommendation to develop long-range plans for the VNS and its management.

To close this recommendation, please provide us with: (1) a copy of the next VNS contract, when available, which includes a plan for periodic replacement of hardware and software; (2) evidence of how ideas that came out of the September 2007 meeting have been used to plan for the future; and (3) a copy of EOUSA's written succession plan for VNS program management.

7. **Resolved.** In its response to our draft report, EOUSA concurred with our recommendation to work with VNS-participating agencies to develop and implement a nationwide procedure for addressing undeliverable correspondence and e-mail.

   To close this recommendation, please provide us the portion of the next VNS contract, when available, containing a technical solution to the issue of returned e-mail notices. Additionally, please provide evidence of how EOUSA is working with other agencies to develop a nationwide policy regarding returned mail.

8. **Resolved.** EOUSA agreed with our recommendation to improve Call Center automated assistance to allow callers to reach an operator at any point during a call. Further, EOUSA stated that an engineering change to allow this access will be considered for a future release to the VNS.

   To close this recommendation, please provide evidence of the engineering change to the VNS, which will allow callers to reach an operator at any point during a call to the VNS Call Center.

9. **Resolved.** In its response to our recommendation to follow up with its contractor to fulfill its requirement to have a Spanish-speaking operator available during all hours of operation, EOUSA stated that the VNS Project Manager has discussed this issue with its contractor. EOUSA further advised that it has developed an interim plan that makes use of another department of the contractor that provides Spanish translations. EOUSA stated this is a temporary solution until additional Spanish-speaking operators can be hired.

   To close this recommendation, please provide us with evidence of the steps the contractor is taking to recruit Spanish speakers and, when it occurs, evidence that these employees have been hired.

10. **Resolved.** EOUSA concurred with our recommendation to work with the United States Marshals Service (USMS) to ensure that

the accurate custody status of defendants is available to victims utilizing the VNS. Moreover, EOUSA stated that it is in contact with the USMS regarding this issue and plans to have VNS ready to accept USMS data by March 2008.

To close this recommendation, please provide us with evidence that the interface between the VNS and the USMS that will allow the VNS to accept USMS custody status data has been developed and is functioning.

11. **Resolved.** In its response to our draft report, EOUSA stated that it will review the VIS regarding the consistency of restitution information and availability.

To close this recommendation, please provide evidence of EOUSA's review of restitution information available in the VIS. This review should provide details of EOUSA's review, including an examination of the consistency of the information and directions provided.

12. **Resolved.** EOUSA concurred with our recommendation to work with VNS-participating agencies to develop a requirement for federal VNS users to record a reason for opting a victim out of the VNS.

To close this recommendation, please provide us, once developed, with documentation of the engineering change request that will require users to select one of the opt-out reasons when electing to stop notifications to a registered victim. Additionally, please provide us evidence that this function has been implemented.

13. **Resolved.** EOUSA concurred with our recommendation and is in the process of implementing data integrity checks and encryption procedures to ensure that transmitted data from the BOP and FBI are complete and accurate, as required by Department policy.

To close this recommendation, please provide evidence (e.g., screen shots and approved change control sheets) that data integrity checks and encryption of transmitted BOP and FBI data files are being performed for the VNS.

14. **Resolved.** EOUSA concurred with our recommendation and stated that it has updated the VNS's system security plan to

include accurate user identification and authentication security information.

To close this recommendation, please provide us a copy of the updated system security plan.

15. **Resolved.** EOUSA concurred with our recommendation and plans to ensure that a disclaimer notification is developed for the VIS application to notify users when they are about to visit a third-party website through a hyperlink.

    To close this recommendation, please provide evidence (such as screen shots and approved change control sheets) that this disclaimer notification has been implemented for the VIS.

16. **Resolved.** EOUSA concurred with our recommendation to modify the VIS application to protect against common web attacks. EOUSA plans to assess the VIS application with a leading commercial web application vulnerability assessment tool and implement corrective actions as appropriate.

    To close this recommendation, please provide EOUSA's VIS vulnerability assessment results and evidence that corrective actions have been implemented.

17. **Resolved.** In response to our recommendation, EOUSA stated that is has completed actions to terminate unnecessary or vulnerable services identified on the VNS servers.

    To close this recommendation, please provide evidence that these actions have been completed.

18. **Resolved.** EOUSA concurred with our recommendation and stated that application and server patches are applied timely. However, EOUSA indicated that not all patches are applied due to technical and business considerations. Furthermore, EOUSA plans to continue to apply selected patches in accordance with documented VNS configuration management processes.

    To close this recommendation, please provide evidence that application and server patches are applied in a timely manner in accordance with Department policies. EOUSA should ensure that approved waivers from the Department are maintained for those patches that are not applied. Additionally, the risks associated

with the vulnerabilities for failure to apply the patches should be approved and documented within the VNS's risk assessment.

19. **Resolved.** EOUSA concurred with our recommendation to adequately secure network devices and server configurations. As a result, EOUSA also plans to regularly assess the VNS's infrastructure using the Department's standard assessment tool. Furthermore, EOUSA indicated that some vulnerabilities listed in Appendix X are now identified by their officials as being false positive. However, EOUSA was presented with the vulnerability assessment results performed by our auditors during the course of the audit, but did not identify any of the vulnerabilities as being false positive.

    To close this recommendation, please provide evidence that EOUSA has adequately secured network devices and server configurations for vulnerabilities identified in Appendix X. EOUSA should also provide evidence of the compensating controls used for those vulnerabilities listed in Appendix X that EOUSA has recently identified as false positive.