Privacy Impact Assessment
for the
Victim Notification System

Certifications:

I certify that this Privacy Impact Assessment conforms to the principles of OMB Memorandum M-03-22, and that the assessed system is in compliance with Section 208 of the E-Government Act of 2002 (Pub. L. 107-347).

/signed/  5/16/2006
Kurt Shernuk  Date
Program Manager, Victim Notification System
Assistant United States Attorney, District of Kansas
U.S. Department of Justice

/signed/  5/24/2006
Dan Villegas  Date
System Owner, Victim Notification System
Counsel, Office of Legal Programs and Policy
Executive Office for United States Attorneys
U.S. Department of Justice

/signed/  5/31/2006
William G. Stewart, II  Date
Acting Assistant Director, Freedom of Information & Privacy Staff
Executive Office for United States Attorneys
U.S. Department of Justice

/signed/  6/1/2006
David W. Downs  Date
Acting Chief Information Officer
Executive Office for United States Attorneys
U.S. Department of Justice
**System Description:** The Victim Notification System (VNS) provides information to victims of federal crime. The notification consists of keeping victims apprised of the status of the investigation of a crime, subsequent stages of the case criminal justice system, and the location and status of an offender while incarcerated or released.

The VNS is currently operational.

**System Purpose:** VNS was created to meet statutorily-imposed responsibilities regarding notification of activity in cases involving victims of federal crime. The Victim and Witness Protection Act of 1982, the Crime Control Act of 1990, the Violent Crime Control and Law Enforcement Act of 1994, the Crime Victims Rights Act (2004) and the Attorney General's (AG) Guidelines for Victim and Witness Assistance set forth procedures to meet the needs of victims of crime. A component of each of these directives is to ensure victims are advised of the significant stages in the criminal justice process and the procedural developments.

In the course of serving this purpose, the VNS must collect and maintain certain personal information which identifies victims of crime.

**Assessment:**

1. **What information is to be collected?**
   a. The information maintained by VNS regarding victims is the same as collected prior to the implementation of the System. The personal information collected and maintained by VNS is:
      i. Full name
         (1) If an organization is the victim, an account number relevant to the loss is collected
      ii. Complete address information for both home and work. Including,
         (1) address, phone, cell phone, email address, fax number, pager number.
      iii. If available,
         (1) Date of birth
         (2) Date of the incident involving the victim
         (3) Date of victims death
         (4) Social security number (required for restitution payments)
         (5) Race
         (6) Gender
         (7) Physical Disabilities
         (8) Do they require protection from the defendant in the case
         (9) Special Circumstances (Child Abuse, Child Exploitation, etc.)
2. Why is the information being collected?

   a. In order to provide notifications required to victims, the information listed in section 1(a) (i) and (ii) above must be maintained to contact the victims. The contact information is collected during the criminal investigation and prosecution of a case. The information in section 1(a)(iii) is used to aid the agency staff in their contact with the victims and/or to assist in identifying groups of victims in larger cases who may require separate notifications.

3. What is the intended use of the information?

   a. The personal information is necessary to notify victims of events pertinent to the investigation, prosecution, and/or incarceration of convicted defendants in their case. In addition, since victims are often witnesses during the prosecution of a case, the information is used to contact the witnesses.

4. With whom will the information be shared?

   a. Access to VNS is limited to authorized users of the System. Outside of the government agencies participating in the investigation, prosecution and incarceration of the defendants, the victim information may be provided to defense counsel as required by the Federal Rules of Criminal Procedure.

5. What opportunities will individuals have to decline to provide information or to consent to particular uses of the information, and how individuals can grant consent?

   a. Most frequently, the information regarding the victims is found during the criminal investigation of the case. Since victims are almost always potential witnesses in a case, their contact information is important to the case being carried forward and the subject of independent discovery by the investigating agency if they decline to make it available. The contact information is not shared outside those responsible for the investigation, prosecution, or incarceration, except as provided by the Federal Rules of Criminal Procedure. While victims cannot
decline to be identified as such, they are able to decline the notification services
provided by VNS. However, their contact information does, as general rule,
remain in the System.

6. **How will the information be secured?**

   a. The information is secured with management, operational, and technical controls
      as delineated by NIST Special Publication 800-53 *Recommended Security
      Controls for Federal Information Systems*. The applied system category control
      set is **moderate** as defined by NIST Special Publication 800-60 *Guide for
      Mapping Types of Information and Information Systems to Security Categories*.
      The system is certified and accredited for control compliance as well as adherence
      to industry security best practices and mitigation of risk due to technical
      vulnerabilities.

   b. The potential risk for unauthorized disclosure of personal information is mitigated
      by
      
      i. limiting the number of authorized system users
      ii. performing background investigations on candidate users
      iii. providing initial and annual system security training
      iv. limiting physical access to the system
      v. robust malicious software management
      vi. timely installation of security patches
      vii. monitoring network activity with an continuously monitored intrusion
           detection System, and
      viii. encrypting personal data during transmission.

7. **Is the system of records being created under the Privacy Act, 5 U.S.C. 552a?**

   a. Yes. The information collected and maintained by VNS is governed by the
      Privacy Act. The information may be disclosed without the individual's consent,
      but only as permitted by the Privacy Act, the Freedom of Information Act, the
      Federal Rules of Criminal Procedure and in accordance with established VNS
      policy and procedure.