Office of Justice Programs

Privacy Impact Assessment
for the
National Missing and Unidentified Persons System
(NamUs)

<u>Issued by:</u>
Maureen Henneberg

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: August 14, 2018

(May 2015 DOJ PIA Template)

EXECUTIVE SUMMARY

The Office of Justice Programs (OJP), a component of the United States Department of Justice (Department or DOJ) operates the National Institute of Justice's (NIJ) National Missing and Unidentified Persons System (NamUs). The purpose of NamUs is to house records and information, without charge, in a centralized location about cases of missing persons, unidentified persons (decedents), and unclaimed persons (decedents), and by permission, based upon access privileges, makes that information available to the general public, law enforcement professionals, coroners, and medical examiners to help solve such cases. Law enforcement, coroners, other professional users add information to the system, with their contact information for other law enforcement or professional users, or members of the public, who have additional information about the missing or identified persons to contact them. In addition, medical examiners, coroners, and law enforcement professionals ("Professional Users") can enter and securely house forensic information such as dental records and fingerprints in NamUs that can be searched by other Professional Users. Some states, such as New York, New Jersey, Connecticut, and Tennessee require the use of NamUs to help solve cases involving missing, unidentified or unclaimed persons.

The NamUs system has conducted this PIA to ensure sufficient protections for the privacy of personal information it collects about missing persons (MP), unidentified persons (UP), unclaimed persons (UCP), general public, Professional Users, and internal OJP users.

NamUs collects and maintains information in identifiable form (IIF) such as: case numbers, names, dates of birth, demographic information (such as race, and ethnicity), physical description, photographs, biometric information (dental and fingerprints), reference numbers to DNA information available from external agencies and labs, family contact information, Social Security Numbers (SSN) (of missing persons only available to Professional Users), work-related data (Professional and OJP internal users only), and investigating agencies contact information. The complete list of information collected is specified in Section 1(c).

Users, based on access privileges, have different levels of access to information in NamUs. See section 1(c) below for a complete listing of NamUs user access privileges.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;

(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

(a) The purpose of NamUs is to house records and information in a centralized location about cases of missing persons, unidentified persons (decedents), and unclaimed persons (decedents), and by permission, based upon access privileges, makes that information available to the general public, law enforcement professionals, coroners, and medical examiners to help solve such cases.

NamUs operates by providing an Internet-based case management and data sharing repository without charge where missing persons, unidentified persons (decedents), and unclaimed persons (decedents) case information can be entered and searched by medical examiners, coroners, and law enforcement professionals ("Professional Users"), and the general public to help solve missing and unidentified person cases. As to the general public, however, only registered users can input information ("Register General Public"). OJP employees, contractors, and grantees (currently the University of North Texas (UNT) Health Science Center (UNTHC) ("Internal Users") also have access to NamUs.

(b) Professional User and Registered General Public users, based on access privileges, can enter information as follows:

Missing Person (MP) case information can be entered by anyone registered. All case information is vetted by the appropriate criminal justice agency prior to it being "published" (i.e., made available or responsive to searches) in NamUs. To be published in NamUs, a local, state, tribal, or federal criminal justice agency must confirm the missing person report, provide a National Crime Information Center (NCIC) and/or law enforcement case number, and give permission to publish the case in NamUs.

Unidentified Person (UP) case information can only be entered by registered medical examiners, coroners, or their authorized designees. These cases involve decedents whose identities are unknown to the investigating agency due to the lack of identification found with the body, or decomposition that precludes visual or fingerprint identification, etc.

Unclaimed Person (UCP) case information can only be entered by registered medical examiners, coroners, or their authorized designees. These cases involve decedents who have been identified by name, but next of kin have not been located in order to make death notifications and/or have the decedent's remains claimed for burial or other disposition.

Once Professional User or Registered General Public users input case information, users can access information, based on access privileges, to assist the users in identifying or resolving MP, UP, and UCP cases. The NamUs system includes algorithmic search capabilities that compares MP/UP/UCP case information and facilitates user-defined advanced searches of the system to locate potential matches.
Advanced searches of NamUs case data may be based on location, demographic information, circumstances, physical and medical characteristics, and other unique metadata.

Professional Users can also enter and securely house forensic information such as dental records, fingerprint records, and other forensic documents or images that can be searched by other authorized Professional Users. Professional Users may choose to share law enforcement sensitive (LES) information with other Professional Users by entering that information into secure areas of NamUs that are not visible to public users. Registered General Public users can enter case information with a limited number of non-LES data sets that are vetted by Regional System Administrators (RSA) before being published. RSAs are programmatic system administrators that assist NamUs users with entering new cases, enhancing data on existing cases, and facilitating requests for forensic services. RSAs also review NamUs case entries for completeness and ensure that only appropriate information will be published.

(c) NamUs collects, maintains, and uses the following types of information related to MP, UP, UCP cases and makes such information available:

To Non-Registered General Public (only MP case information):

- Demographics (age, name, alias, race, gender, height and weight)

To Registered General Public:

- case number – only National Center for Missing and Exploited Children (NCMEC) case number
- demographics (age, name, alias, gender, race/ethnicity, height, and weight)
- circumstances (last known location, date of last contact, circumstances of disappearance, case created date, and case status)
- physical description (hair color, head/body/facial hair description, eye color, eye description (eye shape, wears glasses or contacts), and distinctive physical features)
- clothing and accessories
- vehicle and transportation information (including vehicle make, model, year, style, color, tag number, state, and expiration year; and comments about other modes of transportation, including airline, train, and bus tickets, etc.)
- investigating agency information (investigator name and title, investigating agency name, case number, and date reported)

- photographs (provided that the case owner or contributor has elected to make the image publicly-viewable (vetted by NamUs Regional System Administrators to ensure such photographs do not contain information that is not appropriate for public consumption)).

To Professional and Internal Users:

- case numbers -National Crime Information Center (NCIC) and Violent Criminal Apprehension Program (ViCAP) case numbers
- sensitive demographics information (maiden name, date of birth, place of birth, and blood type)
- SSN (for missing persons cases only and only to Professional Users)
- circumstance notes that are not made public, medical data (free form text entered for one or more following categories – known allergy, skeletal information, known illness, medical implant, medication, drug of abuse, prior surgery, organ absent, foreign object, medical condition/disorder, and other medical information)
- biometrics information
    - DNA: The NamUs system does not include DNA records but indicates only whether such records are available to Professional Users and 1.) whether the records and DNA samples belong to the missing individual, father, mother, sisters, brothers, sons, daughters, or other related individuals; and 2.) whether the samples were submitted to laboratory, and if so, which laboratory and whether the lab results are available.
    - Fingerprints: Fingerprint information that may be collected include the availability and location of fingerprint data, actual fingerprint cards, and corresponding CAFIS or NGI reference numbers, if available.
    - Dental: Dental information that may be collected includes the availability of dental information, to include actual dental records and dentist information such as name, address, email, and phone number.
- information about personal electronic devices which were known, or believed, to be in possession of the individual
- Vehicle Identification Number (VIN)
- investigator phone numbers and email
- family contact information (family contacts name, address, phone number, email, and type of relationship – i.e. father, mother, sister, etc.)
- information about the entering party (a link to user profile that was created by user at the time of registering for access to NamUs application)
- all case attachments that have not been deemed publicly-viewable by the Case Owner or Case Contributor.

(d) Access to the System

The information that users have access to is based on their permission level, including their assigned roles within the system (such as registered public, professional, internal), the status of their agency approval, case ownership, and their regional affiliations.

Public users include members of the public including family members of missing persons, victim advocates, media representatives, and other members of the public who have registered as users on the NamUs application. Registered General Public users have access to information available identified in answer to 1(c) above. Nonregistered public users can conduct a "quick search" based upon first & last name, sex, and state as well as access the following MP case information: first, last, middle name; alias; age; race; sex; height & weight.

Professional Users include law enforcement, medical examiners/ forensic pathologists, coroners, medicolegal investigators, DNA specialists, fingerprint examiners, forensic odontologists, forensic anthropologists, and NCMEC Liaisons. Professional Users have access to information available to Professional Users identified in 1(c) above.

Internal users includes OJP employees, contractors, and grantees (currently the University of North Texas (UNT) Health Science Center (UNTHC). Internal users have access to information available to Professional Users identified in 1(c) above.

(e) Users can search for information in the system using any case datum managed by the system (individually or combined) that the user is authorized to view based on their access level. For example, both general public and Professional Users can perform searches by race, but only Professional Users can perform a search by blood type.

(f) NamUs is a web-based application, and all information transmitted to and from the application happens via secure communication protocol (HTTPS) and DOJ Trusted Internet Connection (TIC).

(g) NamUs does not interconnect with any other system.

(h) NamUs is a major web application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration*	X	Financial account	
Taxpayer ID		Driver's license*	X	Financial transaction	
Employee ID		Passport*	X	Patient ID	
File/case ID	X	Credit card			

Identifying numbers
* The system does not contain field attributes to specifically collect driver's license, passport, and alien registration numbers as these are not data sets within NamUs. Professional Users, however, may enter this information in free-form text if these numbers are considered relevant to the case by the law enforcement agencies. OJP will collect the following identifying numbers about MP: social security. OJP will collect the following identifying numbers about MP, UP, and UCP cases: case number.

General personal data

Name	X	Date of birth	X	Religion	
Maiden name	X	Place of birth	X	Financial info	
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service*	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	X

Other general personal data (specify):

- Height
- Weight
- Blood Type

* Although military information may be entered by armed services divisions that have jurisdiction over the missing and unidentified person cases, no dataset information can be collected specifically for military cases.

OJP will collect the following general personal data about MP, UP, and UCP: name, alias, gender, race/ethnicity, physical characteristics, height and weight, maiden name, date of birth, and medical information (blood type).

OJP will collect the following general personal data about Registered General Public, Professional, and Internal Users: name, telephone number, email address.

Work-related data*

Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates	X		

Other work-related data (specify):
*Note: OJP will collect this information about Professional and Internal Users.

Fingerprints	X	Photos	X	DNA profiles	
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	X

Other distinguishing features/biometrics (specify):

- Hair Color
- Head Hair Description
- Body Hair Description
- Facial Hair Description
- Eye Color
- Eye Description
- Distinctive Physical Features (piercing, amputation, artificial body part, deformity, scar/mark, tattoo, etc.)
- Reference to the availability of DNA (not actual DNA profiles) stored and maintained by external organizations (i.e. labs, criminal justice agencies)

OJP will collect the following distinguishing features/biometric information from the Registered General Public about MP: photos, hair color, head/body/facial hair description, eye color, eye description, and distinctive physical features.

OJP will collect the following distinguishing features/biometric information about MP, UP, UCP from Professional Users: all of the above as well as reference to the availability of DNA.

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run		Contents of files	X

Other system/audit data (specify): NamUs creates an audit record whenever a registered user accesses a case. The audit record only contains user id, case id, and when the case was accessed.

Note: The system administrative/audit data only applies to information about public or professional registered users, but does not apply to public non-registered users.

Other information (specify)	

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual[1] about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government sources					
Within the Component		Other DOJ components	X	Other federal entities	X
State, local, tribal	X	Foreign			
Other (specify):					

Non-government sources					
Members of the public	X	Public media, internet		Private sector	
Commercial data brokers					
Other (specify): • Non-Government Organization (NGO)					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There may be many potential risks when sensitive IIF (including medical information and biometric information) about an individual is collected from multiple sources and recorded. Risks include but are not limited to, abuse of the system by the public by reporting a person as missing although that person has intentionally moved away or sheltered due to domestic violence or other abuses; certain insurance coverage being refused; loss of employment if certain medical information became public; identity theft; and misuse of the collected information by government or contractor personnel. To mitigate the threats to privacy caused by abuse of the system, all case information submitted is vetted and validated with the criminal justice agency that has jurisdiction over the case by a NamUs Regional System Administrators (RSA). Additionally, the criminal justice agency personnel who are part of the sources providing or editing case information including sensitive IIF, are vetted and validated by RSA's to ensure they are employees, contractors, or representatives of the criminal justice agency and they are authorized by the criminal justice agency to enter as well as edit case information.

[1] Individuals mean registered public and Professional Users. It does not include non-registered public users.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): The purpose of the NamUs system is to provide an Internet-based case management system without charge to store data in a centralized repository where relevant and appropriate case information can be entered as well as searched, based upon access privileges within the system, by medical examiners, coroners, and law enforcement professionals (Professional Users), internal users, and the general public to help solve missing and unidentified person cases.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The Office of Justice Program (OJP), NIJ, NamUs maintains information in a centralized location regarding cases of missing persons, unidentified persons, and unclaimed persons, and by permission, based upon role and access privileges, makes the information available to the general public, internal OJP users, as well as law enforcement professionals, coroners, and medical examiners (Professional Users) to help solve such missing and unidentified persons cases. The NamUs system provides an Internet-based case management system without charge to store data in a centralized repository where relevant and appropriate case information can be entered and searched by Professional Users, internal users, and the registered general public to help solve missing and unidentified person cases. NamUs users can search case information in the system using any case attributes they are authorized to view based on their access level. For example, both registered public and Professional Users can perform searches by race, but only Professional Users can perform a search using, for example, blood type.

The NamUs system includes algorithmic search capabilities that compares MP/UP case information and facilitates user-defined advanced searches of the system to locate potential matches. Advanced searches of NamUs case data may be based on location, demographic information, circumstances, physical and medical characteristics, and other unique metadata.

Professional Users can also enter and securely house forensic information such as dental records and fingerprint records that can be searched by other authorized Professional Users. Professional Users may choose to share law enforcement sensitive (LES) information with other Professional Users by entering that information into secure areas of NamUs that are not visible to public users. Registered public users can enter case information with a limited number of non-LES data sets that are vetted by Regional System Administrators (RSA) before being published. RSAs are programmatic system administrators that assist NamUs users with entering new cases, enhancing data on existing cases, and facilitating requests for forensic services. RSAs also review NamUs case entries for completeness and ensure that only appropriate information will be published.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	• Title I of the Omnibus Crime Control and Safe Streets Act of 1968 (sections 201 and 202); • Homeland Security Act of 2002 (section 232); and 28 U.S.C. 530C. • Various state statutes as some states have laws requiring Professional Users to enter missing or unidentified person cases into the NamUs system.
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The retention period for the NamUs system is pending. Until the National Archives and Records Administration approves the retention and disposal schedule, records will be treated as permanent.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users

regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

OJP has worked to mitigate the privacy risks associated with the use of the information. There may be many potential risks with the use of the information such as identity theft or misuse of the collected information by government and contractor personnel, etc. To ensure the information is handled, retained, and disposed appropriately, OJP has put the following controls into place:

• A DOJ background check is performed on all DOJ personnel, including employees, and contractors working on NamUs. In addition to background check, all DOJ personnel are required to complete annual computer security awareness training and sign "DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" that includes rules for safeguarding identifiable information.
• All law enforcement Professional Users are vetted and validated by RSA's before they are granted permission to add and edit cases as Professional Users. The vetting and validation done by RSA's is to ensure the law enforcement professionals are employees, contractors, or representatives of actual law enforcement agencies and they are sponsored by their agency to manage cases within NamUs.
• Users of the system can only gain access to the data by a valid user identification and password. Access to the data in the system is further limited by the user's assigned role within the system.
• Internet connections to NamUs are protected by multiple firewalls and the DOJ Trusted Internet Connection (TIC).
• Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations.
• Auditing features of NamUs captures changes to cases, agency profiles, and user account profiles (including sponsorships) that allows for the reconstruction or review of actions taken by an individual including any unauthorized modifications to case data.
• All communications between users and the system are protected by secure communication protocol that provides confidentiality and integrity of the transmitted data.
• System leverages Federal Risk and Authorization Management Program (FedRAMP) compliant cloud service infrastructure with security controls including physical safeguards appropriate for a Federal Information Security Management Act (FISMA) system categorized by information technology personnel as "moderate," that means an application of security and privacy controls to protect the information and information systems taking into account OJP and DOJ's level of concern for confidentiality, integrity, and availability as well as the potential impact on its assets and operations should the information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X		X	
DOJ components	X		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public	X		X	
Private sector				
Foreign governments				X
Foreign entities				
Other (specify): Non-Government Organization (NGO) (direct access) and media per FOIA on a case-by-case	X		X	

Note: Regarding direct access, authorized employees, contractors, and registered users (including law enforcement professionals) will have limited direct data access dependent upon their assigned roles and privileges within the system.

<u>Within the component:</u>

Information, as appropriate, is shared within the Office of Justice Programs (OJP) for purposes of system development and maintenance, auditing, communication and outreach, program oversight, and research.

- NIJ NamUs Program Staff – Public and non-public information
- NIJ Research Staff – With permissions public and non-public information on a limited case-by- case basis
- OJP Office of the Chief Information Officer – Public and non-public information
- OJP Office of the General Counsel
- OJP and NIJ Office of

Communications <u>DOJ components:</u>

Information, as appropriate, is shared within the Department for purposes of communication and outreach, sharing case related information and program oversight.

- DOJ Leadership

- DOJ Office of the Assistant Attorney General
- DOJ Office of Communications
- DOJ Office of Privacy And Civil Liberties
- Federal Bureau of

Investigation Federal entities:

Information, as appropriate, is shared with Federal Public Safety agencies, such as the Federal Bureau of Investigation or the Armed Services Divisions, for communication and outreach as well as sharing case related information.

State, local, tribal gov't entities:

Information, as appropriate, is entered, searched, and shared with state, local, and tribal Professional Users, without charge, either voluntarily or by state statute to help solve missing and unidentified person cases.

Foreign Entities:

Information, as appropriate, is searched and shared with foreign governments such as Mexico and Canada.[2] Foreign entities are not allowed to register in NamUs and therefore, can only conduct a "Quick Search" for MP by entering a "First name" "Last name" "Sex" and "State" information to retrieve MP Case Information (Names, NCMEC Number (if applicable), Date Last Seen, Age Last Seen, Age Now, Race, Ethnicity, Sex, Height, and Weight).

Non-governmental Organization:

Information, as appropriate, is entered, searched, and shared with non-governmental organizations such as the National Center for Missing and Exploited Children and other Child Advocacy Organizations to help solve missing and unidentified person cases.

General Public:

Information, as appropriate, is entered, searched, and shared with the general public to help solve missing and unidentified person cases. Only registered public users, however, can input and share information regarding MP and UP cases. Non-registered public users can conduct a "Quick Search" by entering a "First name" "Last name" "Sex" and "State" information to retrieve only MP Case Information (Names, NCMEC Number (if applicable), Date Last Seen, Age Last Seen, Age Now, Race, Ethnicity, Sex, Height, and Weight).

Information, as appropriate, is also shared with the public for purposes of complying with the Freedom of Information Act, unless the information, if disclosed, would invade an individual's privacy, or another FOIA exemption applies.

---

[2] As these countries have common boundaries they have searched NamUs for MP cases. Other foreign countries may also access NamUs to locate MP as non-registered public users. Foreign entities cannot register in NamUs.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

To reduce the risk to privacy, case data is shared on a case-by-case basis through direct access via NamUs as listed in section 4.1. The following controls have been put into place in order to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient:

• The direct access via NamUs provided to law enforcement professionals, public and DOJ employees and contractors are with access controls that is commensurate with their purpose of access.
• All law enforcement professionals are vetted and validated by RSA's before they are granted permission to add cases and/or edit case information as Professional Users. The vetting and validation done by RSA's is to ensure the law enforcement professionals are employees, contractors, or representatives of their law enforcement agency and they are sponsored by their agency to manage their cases with NamUs.
• A DOJ background check is performed on all DOJ personnel, including employees, and contractors working on NamUs. In addition to background check, all DOJ personnel are required to complete annual computer security awareness training and sign "DOJ Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" that includes rules for safeguarding identifiable information. Medical Reviewers are required to sign non-disclosure agreements.
• Users of the system can only gain access to the data by a valid user identification and password. Access to the data in the system is further limited by the user's assigned role within the system.
• Auditing features of NamUs captures changes to cases, agency profiles, and user account profiles (including sponsorships) that allows for the reconstruction or review of actions taken by an individual including any unauthorized modifications to case data.
• All communications between users and the system are protected by secure communication protocol that provides confidentiality and integrity of the transmitted data.
• Internet connections to NamUs are protected by multiple firewalls and the DOJ Trusted Internet Connection (TIC).
• Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations.
• System leverages FedRAMP compliant cloud service infrastructure with security controls including physical safeguards appropriate for a FISMA moderate system.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: In addition to the system of records notice being published in the Federal Register, the Privacy Act (e)(3) statement is displayed by the system as a link entitled "Privacy Act Notice" at the time of user login and the system also has a permanent link to the statement that is available to the user at all times at the bottom of the screen as a footer entitled "Privacy Act Notice."
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

The following individuals[3] have the opportunity to decline providing information in

NamUs: Public Users: individuals who can voluntarily opt in or out of using NamUs.
Professional Users: individuals in states where NamUs is voluntary and not required by law.

The following individuals do not have the opportunity to decline providing information in NamUs:

Professional Users: in States where NamUs is not voluntary but required by State law. At the time of publication this includes States such as New York, New Jersey, Connecticut, and Tennessee.

Missing Persons: individuals who are unavailable to provide consent.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Please see explanation above.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Please see explanation above.

[3] For purposes of the Privacy Act, "individuals" do not include deceased or unclaimed persons given that the Privacy Act protections generally do not apply to deceased individuals.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

The following individuals have the opportunity to consent to particular uses of information:

Public Registered and Professional Users: when registering and logging into NamUs are presented with a link to "Privacy Act Notice." The notice states "Effect: Providing information in the NamUs system is voluntary" and can (or not), therefore, consent to the uses of information.

The following individuals do not have the opportunity to consent to particular uses of information: Missing Persons: individuals who are unavailable to provide consent.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Please see explanation above.
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Please see explanation above.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Users are presented with a link to a "Privacy Act Notice" specifying the authority for OJP to solicit the information, purpose (to help solve MP, UP, and UCP cases), routine uses, and the disclosure of such information is voluntary The link to the Privacy Act Notice is provided at the time of login and displayed prominently as a hyperlink on the screen where the user begins the process for submitting the case data. Users are also provided with a link to the Privacy Act Notice on all pages in the footer section of the website.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: Expected completion date: 05/10/2018
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Required controls for a Federal Information Security Modernization Act (FISMA) moderate system and DOJ Cybersecurity Standard (Unclassified Security Control Matrix) have been identified, implemented, and assessed for NamUs.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: During the development of the system, the user stories (i.e., high level system requirements) are tested to ensure they are functioning as intended, including safeguards for the information. Additionally, OJP has implemented IT Security continuous monitoring, a critical part of risk management process, where security controls and risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately safeguard the information.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: The system's auditing features enable reconstruction or review of actions taken by an individual including unauthorized modification or misuse of information. Auditing includes changes to the case data and events related to user access.
X	Grantees that have access to the system are subject to provisions in their grant award binding them under the Privacy Act as follows: The award recipient agrees, as a condition of award approval, to comply with the requirements of 28 CFR Part 22, including the requirement to submit a properly executed Privacy Certificate that is in compliance with 28 CFR § 22.23 to the National Institute of Justice for approval.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy. *See OJP Clause No. OJP 2852.204-78.*
X	The following training is required for authorized users to access or receive information in the system:

	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.

	X	Other (specify):	General information security training for authorized users within OJP.

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Internet connections are protected by multiple firewalls. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensics analysis during incident investigations. Users of the system can only gain access to the data by a valid user identification and password. Access to the data in the system is further limited by the user's assigned role within the system. Changes to the case data are audited in the system that enables the reconstruction or review of actions taken by a user including unauthorized modifications to the case data. All communications between users and the system are protected by secure communication protocol and the DOJ Trusted Internet Connection (TIC) which provide confidentiality and integrity of the transmitted data. System leverages FedRAMP compliant cloud service infrastructure with security controls including physical safeguards appropriate for a FISMA moderate system. All DOJ personnel, including the employees and contractors with access to NamUs, are required to complete annual security awareness training and adhere to Rules of Behavior that includes rules for safeguarding Personally Identifiable Information.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: National Missing and Unidentified Persons System (NamUs), Justice/OJP-015, 83 FR 13306 (March 28, 2018)
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Users can search for MP, UP, and UCP information in the system using any case datum managed by the system (individually or combined) that the user is authorized to view based on their access level. NamUs does not generally retrieve information about United States citizenship or lawful admitted permanent residency given its stated purpose.