



## **National Institute of Justice**

## **National Missing and Unidentified Persons System (NamUs)**

## **Policy Manual**

### **Version 1.0**

*Last Updated February 11, 2014*

*This Policy Manual will be periodically reviewed and may be updated at any time at the discretion of the National Institute of Justice.*

Approved:

National Institute of Justice

Mr. Charles Heurich

Date: \_\_\_\_\_ Initials: \_\_\_\_\_

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### Table of Contents

1.00	Concept of NamUs Operations .....	5
1.01	Overview of NamUs .....	5
1.02	Program Funding and Management .....	5
2.00	NamUs Policy Manual .....	7
2.01	Purpose of NamUs Policy Manual .....	7
2.02	Access for External Personnel .....	7
2.03	Approval Requirements for Changes to the NamUs Policy Manual .....	7
3.00	Overview of the NamUs Databases .....	8
4.00	NamUs Forensic Subject Matter Expert (SME) Assistance .....	9
5.00	NamUs Forensic Reporting .....	9
5.01	Report Control .....	10
5.02	Expert Witness Testimony .....	10
5.03	Travel Expenses Related to Testimony .....	10
6.00	Personally Identifiable Information .....	11
6.01	Definition of Personally Identifiable Information .....	11
6.02	Addressing and Safeguarding PII .....	12
7.00	Freedom of Information Act (FOIA) Requests .....	13
7.01	Overview of the Freedom of Information Act .....	13
7.02	Requirements for FOIA Requests .....	13
7.02.1	Criminal Justice Agency FOIA Requests .....	13
7.02.2	Public FOIA Requests .....	14
7.02.3	FOIA Submission Process .....	14
8.00	NamUs Staff .....	17
8.01	Personnel Contact List .....	17
8.02	NamUs Regional System Administrator Assignment Map .....	18
8.03	NamUs Forensic Odontologist Assignment Map .....	19
9.00	Regional System Administrator Responsibilities .....	20
9.01	The Role of the RSA .....	20
10.00	General User Registration Issues .....	21
10.01	Terms of Use .....	21

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

10.02	User Approval.....	21
10.03	Required Information.....	21
10.04	User Roles and General Vetting Issues .....	22
11.00	User Permission Levels – MP/UP/UCP Databases .....	23
11.01	Criminal Justice Agency Users and Permissions.....	23
11.02	Forensic Anthropology/Pathology Users .....	24
11.03	Military/Federal Criminal Justice Users .....	24
11.04	Specialized CJA Users: Forensic Subject Matter Experts .....	24
11.05	NamUs Administration/Staff.....	25
11.06	Grandfathered User Categories .....	25
12.00	Vetting New NamUs User Registrations .....	26
13.00	MP/UP/UCP User Renewals.....	28
13.01	User Renewal Cycles .....	28
13.02	Responding to Renewal Requests.....	28
13.03	Users No Longer Sponsored for Access to NamUs Databases .....	29
13.04	Revalidation/Renewal of User Account .....	29
14.00	Case Owners/Managers.....	31
14.01	Roles and Responsibilities.....	31
14.02	Case Owner/Case Manager Permissions .....	31
15.00	NamUs MP/UP/UCP Volunteer Users.....	32
15.01	UNTCHI Forensic Services Unit.....	32
15.02	Volunteer Concept/Vetting Process .....	32
15.03	Volunteers with Existing Elevated Permissions to UP/MP Databases .....	32
16.00	Entry, Acceptance and Publication of Cases in NamUs .....	34
16.01	Manual Case Entry .....	34
16.02	Electronic Data Crosswalk Protocols.....	34
16.03	Minimum Mandatory Case Data.....	34
16.04	“Pending” NamUs Case Statuses .....	36
16.05	Case Publication .....	36
17.00	Unverifiable Cases.....	39
17.01	Unverifiable MP Cases .....	39
17.02	Unverifiable UP Cases: .....	42

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

17.03	Unverifiable UCP Cases:.....	42
18.00	NCMEC Case Selection Criteria .....	43
18.01	Assignment of MP Cases to National Center for Missing and Exploited Children (NCMEC) ..	43
18.02	Reassignment of MP Cases Not Publishable by NCMEC.....	44
18.03	Assignment of UP Cases to NCMEC RSAs.....	44
18.04	Assignment of UCP Cases to NCMEC RSAs.....	46
19.00	NEIM / XML Exchanges .....	47
	Glossary.....	48

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 1.00 Concept of NamUs Operations

##### 1.01 Overview of NamUs

The National Missing and Unidentified Persons System (NamUs) is a clearinghouse for information related to missing person, unidentified decedent and unclaimed person cases across the United States, as well as a system of forensic and analytical resources to help resolve these cases. The NamUs databases, located online at [www.namus.gov](http://www.namus.gov), are free, Internet-based data repositories that can be searched by medical examiners, coroners, law enforcement personnel and the general public to help solve missing and unidentified person cases.

When a new missing or unidentified person case is entered into the NamUs database and validated, the system automatically performs comparisons, searching for matches or similarities between missing and unidentified persons. Most registered NamUs users – including law enforcement personnel, medical examiners, coroners, and case managers – are able to view system-generated matches and adjust matching criteria to filter results. In addition, users can perform manual searches of the NamUs databases to locate potential matches based on unique features such as scars, marks, tattoos, jewelry and clothing descriptions, etc.

In addition to case support and investigative analysis, NamUs also provides access to free forensic services, including DNA analyses, anthropology, odontology and fingerprint examinations.

##### 1.02 Program Funding and Management

NamUs is funded and overseen by the National Institute of Justice (NIJ) and managed through a cooperative agreement with the University of North Texas (UNT) Health Science Center (award number 2011-MU-BX-K063). Additional access to forensic services is provided through a separate cooperative agreement under the 2012 Missing Persons Award (award number 2012-DN-BX-K057).

Within the UNT Health Science Center, Center for Human Identification (ORI # TX220035Y), NamUs management is divided into two divisions – the Operations Division and the Training and Analysis Division – with additional resources and support provided by the UNT Health Science Center’s Information Technology Services (ITS) Department and the Center for Human Identification’s Forensic Services Unit, Laboratory for Forensic Anthropology and Laboratory for

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

Molecular Identification. The program management team performs the overall coordination of NamUs activities, ensuring that operations run smoothly for all NamUs stakeholders. The NamUs organization is structured so that all roles report and communicate to the program management, with ultimate oversight by NIJ, thus providing a cohesive operation for both UNTCHI and NIJ.

## 2.00 NamUs Policy Manual

### 2.01 Purpose of NamUs Policy Manual

The NamUs Policy Manual defines current roles for NamUs stakeholders, communicates system characteristics, and provides descriptions of how NamUs capabilities may be employed to achieve the objectives of the system. The NamUs Policy Manual provides a clear methodology for meeting the goals of the NamUs program through the following topics:

- Strategies and policies affecting the system
- Clear statement of responsibilities and delegation of authorities
- Specific processes for operating the system

### 2.02 Access for External Personnel

An open-access, read-only copy of the NamUs Policy Manual is available on the “About NamUs” page that can be accessed at [www.NamUs.gov](http://www.NamUs.gov). The NamUs Policy Manual will be periodically reviewed and may be updated at the discretion of the National Institute of Justice. A current version of the NamUs Policy Manual will be posted to [www.NamUs.gov](http://www.NamUs.gov) if/when updates are made.

### 2.03 Approval Requirements for Changes to the NamUs Policy Manual

Requested changes to any existing NamUs Policy Manual section will be reviewed and approved by all NamUs senior management members prior to any changes being implemented, with the express approval of NIJ. Requests for changes may be submitted to NamUs senior management by any NamUs or National Institute of Justice staff member.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 3.00 Overview of the NamUs Databases

NamUs contains three databases related to Missing Persons (MP), Unidentified Persons (UP) and Unclaimed Persons (UCP). All NamUs databases can be accessed from [www.NamUs.gov](http://www.NamUs.gov). The NamUs databases can be searched by criminal justice agencies (CJAs) and members of the general public, in hopes of resolving cases.

The NamUs **Missing Person (MP) Database** contains information related to missing persons that can be entered by anyone; however, before a missing person case is published for public viewing, it must be vetted with the appropriate CJA and that agency must provide NamUs with permission to publish the case. The NamUs MP database provides users with a variety of resources; including the ability to print missing person posters, receive free biometric collection assistance and search the NamUs databases for potential associations between missing, unidentified and unclaimed persons. The NamUs MP database can be accessed directly from [www.FindTheMissing.org](http://www.FindTheMissing.org).

The NamUs **Unidentified Person (UP) Database** contains information related to decedents whose bodies have not been identified, as well as living persons whose identity is unknown due to memory impairments and/or other circumstances. UP cases are entered by medical examiners and coroners and their designees throughout the United States. NamUs allows all stakeholders to search the UP database using a variety of distinct features or advanced search options, including characteristics such as sex, race, distinct body features, dental information, etc. The NamUs UP database can be accessed directly from [www.IdentifyUs.org](http://www.IdentifyUs.org).

The NamUs **Unclaimed Person (UCP) Database** contains information related to deceased persons who have been identified by name, but for whom no next of kin has been identified or located to claim the body for burial or other disposition. UCP cases can be entered only by CJAs and their designees, but the database is searchable by the public. Once next of kin has been located and verified by the case owner, cases should be removed from public view unless there is an investigative reason to do otherwise. The NamUs UCP database can be accessed directly from [www.ClaimUs.org](http://www.ClaimUs.org).

NamUs is not an official investigative case file or an official report related to missing and unidentified persons. NamUs is only a repository for information entered by users from across the country; a NamUs record may or may not contain complete information about any particular case. Criminal justice agencies may choose to share law enforcement sensitive (LES) information or criminal justice information (CJI) with other criminal justice agencies by entering that information into areas of the system that are restricted from public view. However, agencies may also choose to omit LES information and/or CJI related to a particular case when they deem appropriate.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 4.00 NamUs Forensic Subject Matter Expert (SME) Assistance

##### 4.01 Scope of Subject Matter Expertise

NamUs forensic Subject Matter Experts (SMEs) include specialists in forensic odontology, forensic anthropology, fingerprint examination and DNA analyses.

##### 4.02 Requesting SME Assistance

All cases must be entered into the NamUs Missing Person (MP) or Unidentified Person (UP) database in order to obtain assistance from NamUs SMEs. Requests for SME assistance can be made directly to the SME, or services may be requested through the NamUs Regional System Administrators. In limited circumstances, biometric services may be provided without a full case entry into NamUs. Prior approval for these services must be obtained by contacting the appropriate NamUs Regional System Administrator or NamUs management.

##### 4.03 SME Guidelines

When SME assistance is requested to obtain, examine, process and/or code biometric information, the SME will:

- Enter all applicable biometric coding into NamUs (e.g., dental coding and AFIS fingerprint codes) for view by approved NamUs criminal justice users or allied professionals.
- Upload all biometric images to NamUs (e.g., dental radiographs and fingerprint cards) for view by approved NamUs criminal justice users or allied professionals. Images submitted to NamUs will be enhanced by the SME *only* to increase resolution/clarity, and/or to remove personally identifying information (e.g., social security number).
- Alterations to any work product entered into NamUs by an SME will not be approved without consultation and approval by the SME.

#### 5.00 NamUs Forensic Reporting

Forensic Odontologists and Fingerprint Specialists employed by the UNT Center for Human Identification (UNTCHI) may prepare forensic reports for criminal justice agencies as they relate to criminal investigations stemming from, or relative to, a missing person or unidentified decedent case for which NamUs supported the CJA.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

Forensic reports will be prepared on a template conforming to UNTCHI's reporting requirements under FQS/IEC 17025 (See appendix for *ANSI-ASQ National Accreditation Certificate*). The body of the report will be prepared by each subject matter expert, who will be responsible for testifying to the content of the report, as appropriate.

#### 5.01 Report Control

For each forensic report prepared by a UNTCHI Forensic Odontologist or Fingerprint Specialist, two copies containing original signatures will be created. One copy of the report will be sent to the appropriate criminal justice agency and one copy of the report will be sent to the NamUs Administrative Assistant for permanent storage. The subject matter expert may retain an additional copy in his/her controlled possession. Release of the reports to outside parties other than the appropriate CJAs or UNTCHI personnel is strictly prohibited. Parties other than the appropriate CJA or UNTCHI personnel requesting copies of forensic reports should be directed to the appropriate CJA.

#### 5.02 Expert Witness Testimony

UNTCHI subject matter experts supporting NamUs may provide one day of expert witness testimony to the appropriate CJA without charge for service. Service means actual testimony or required presence away from the subject matter expert's normal work location. Additional days of service may result in a charge of \$1,000 per day. The additional day of service fees may be waived at the discretion of the NamUs National Director of Operations.

#### 5.03 Travel Expenses Related to Testimony

It will be the responsibility of the CJA or prosecuting authority requesting the subject matter expert to cover all costs associated with travel related to the expert witness testimony. Travel expenses may include airfare, vehicle mileage, parking expenses, hotel accommodations, meals and other related travel expenses.

## 6.00 Personally Identifiable Information

### 6.01 Definition of Personally Identifiable Information

Personally identifiable information (PII) “refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”<sup>1</sup> NamUs has adopted the National Institute of Standards and Technology (NIST) examples of PII<sup>2</sup>, which are listed below with additional examples considered PII by NamUs. This list is not all-encompassing, and the Regional System Administrators (RSA) should use his/her judgment when confronted with additional examples of data that may be considered PII.

- An individual’s full name, maiden name, mother’s maiden name, or alias name(s)
- A personal identification number, such as a social security number (SSN)
- Passport numbers
- Driver’s license numbers
- Taxpayer identification numbers
- Financial accounts or credit card numbers
- Citizenship or immigration status
- Address information, such as a specific street address or Post Office Box
- Email addresses, screen names, IP addresses, or other information that could link a particular individual to an online account or specific geographic location
- Personal characteristics, including photographic images (especially of faces or other identifying characteristics), fingerprints, handwriting, or other biometric data (e.g. retina scan, voice signature, facial geometry).
- An individual’s DNA profile or numbers that would identify an individual’s DNA profile at a criminal justice agency or within the Combined DNA Index System (CODIS)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

---

<sup>1</sup> Executive Office of the President, Office of Management and Budget. “M-07-16 Memorandum for the Heads of Executive Departments and Agencies: Safeguarding Against and Responding to the Breach of Personally Identifiable Information”. Accessed 05-14-2012 from <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf>

<sup>2</sup> National Institute of Standards and Technology (NIST). “Guide to Protecting the Confidentiality of Personally Identifiable Information”. Accessed 05-14-2012 from <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 6.02 Addressing and Safeguarding PII

NamUs staff members and management encounter PII on a daily basis. PII will be present in cases entered into the MP/UP/UCP databases, and PII will be encountered when discussing cases with family members, law enforcement and forensic specialists. It is necessary for certain elements of PII to be released to the public to assist in locating a missing person or identifying an unknown decedent, such as the full name of a missing person or the potential name of an unknown decedent taken from items located with the body. It is the responsibility of all NamUs staff members and management to safeguard PII that might be misused to commit identity theft or other crimes, such as date of birth and social security number, by ensuring that such information is not made available to the public by NamUs, used for purposes other than locating a missing person/relative/associate for investigative reasons, or misused in any other way.

The RSA will review all contents and comments in a NamUs case file to ensure that none of the information that is defined in Section 5.01 of this policy as PII is made viewable to the public. Social Security numbers are **never** to be accepted into the NamUs databases, regardless of whether the data is hidden from public view. It is necessary for some PII to be publicly viewable in order to facilitate a recovery or identification (e.g., full name of missing person). The RSA will use his/her discretion to safeguard and restrict from public view any PII that is not necessary to resolve the MP/UP case and/or can be used to commit identity theft or be misused in some other manner.

Upon locating existing PII in a NamUs MP/UP case – or before publishing a case where PII would become visible to the public – the RSA will contact the investigating CJA and resolve the PII concern by deleting the information, moving the information to a non-public field in the database, or restricting the field from public view. Data entered by a CJA will be deleted, moved or restricted from public view *only* after contacting the agency which owns the case. If a case has been entered by a member of the general public and has not yet been vetted by a CJA, information may be moved to non-public sections of NamUs prior to review by a CJA at the RSA's discretion. RSAs will be equally diligent in reviewing MP and UP cases for PII, as the "Circumstances" and other comment fields in each case type may contain PII related to living individuals, such as relatives of missing or unclaimed persons, and persons of interest in UP cases, etc.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 7.00 Freedom of Information Act (FOIA) Requests

#### 7.01 Overview of the Freedom of Information Act

The Freedom of Information Act (FOIA) is a law that gives any person the right to access information from the federal government.

The National Missing and Unidentified Persons System (NamUs) is controlled by the National Institute of Justice (NIJ) under the Department of Justice (DOJ). DOJ is generally required under FOIA to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions and three exclusions contained in the statute. FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public access laws that should be consulted for access to state and local records. Each federal agency is responsible for meeting its FOIA responsibilities for its own records. A list of principal FOIA contacts at federal agencies is available from the DOJ website. Each DOJ component is responsible for processing FOIA requests for the records that it maintains.

More information related to FOIA, including additional FOIA contact information, may be found at the following: <http://www.foia.gov>.

#### 7.02 Requirements for FOIA Requests

Data that can be collected from the NamUs MP/UP/UCP databases using the “Advanced Search” or other features/tools within NamUs, through public access or a user’s vetted, activated NamUs account, **does not** require a FOIA request. Any data that cannot be obtained in this manner, such as requests for data in formats not available through existing NamUs features/tools, will require a FOIA request to be submitted directly to DOJ. All FOIA requests will be reviewed by the Office of Justice Programs (OJP) Office of the General Council (OGC) in accordance with the following guidelines:

##### 7.02.1 Criminal Justice Agency FOIA Requests

CJAs submitting FOIA requests for NamUs data should submit requests to the OJP OGC via an official government email account, or on official agency letterhead via email, fax or mail. All requests should include the following:

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

- Data fields requested in the search results (e.g., MP name, DOB, city missing and state missing).
- Requested search parameters (e.g., all MP cases involving white females last seen in Texas between 01-01-2012 and 12-31-2012).
- Requestor's name and contact information, to include the requestor's agency and role within the agency.

#### 7.02.2 Public FOIA Requests

Members of the public or other non-CJA requestors may submit FOIA requests for NamUs data to the OJP OGC via email, telephone, fax or mail. All requests should include the following:

- Data fields requested in the search results (e.g., MP name, DOB, city missing and state missing).
- Requested search parameters (e.g., all MP cases involving white females last seen in Texas between 01-01-2012 and 12-31-2012).
- Requestor's name and contact information.

#### 7.02.3 FOIA Submission Process

All FOIA requests will be reviewed by the OJP OGC prior to the collection and/or dissemination of any data related to the request. Unless directed otherwise by DOJ and/or the NIJ NamUs Program Manager, all FOIA requests for NamUs data will adhere to the following procedures:

- All requests will be submitted to the OJP OGC in accordance with the guidelines and protocols outlined in Section 5.02 of this NamUs Policy Manual.
- Upon review by OJP OGC and the NIJ NamUs Program Manager, NamUs Senior Management will be notified of any FOIA requests to be processed by NamUs.
- Data will be gathered by the NamUs Training and Analysis Division at the direction of the NIJ NamUs Program Manager. The NamUs Training and Analysis Division may request assistance from the UNT Health Science Center Information Technology Services (ITS) Department in gathering data, developing a secure method of

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

transferring personally identifiable information (PII)/law enforcement sensitive information, etc.

- NamUs Senior Management will disseminate the collected data back to OJP and/or the NIJ NamUs Program Manager for review and further dissemination, if appropriate. Information related to the time spent processing each request will be documented by the Training and Analysis Division and provided with the data results.
- All follow-up questions/requests from the FOIA requestor should be routed through the OJP OGC, which will work in conjunction with the NIJ NamUs Program Manager and/or NamUs Senior Management to develop additional data and/or responses to the requestor, as appropriate.

As CJA requests may involve data that is not publicly viewable, but is authorized for distribution to CJA requestors, any data that is not publicly viewable and is to be returned to a CJA requestor in response to a FOIA request will be disseminated back to the requestor via a secure File Transfer Protocol (FTP) or similar method to be established by NamUs Senior Management in conjunction with OJP and/or the NIJ NamUs Program Manager.

Public users requesting data that is not publicly viewable and/or cannot be viewed using their vetted user profile will be reviewed by OJP OGC and additional contact will be made with these requestors to revise their request and/or deny their request for such data, as appropriate.

All FOIA responses shall be routed through the OJP OGC; NamUs staff members and/or Senior Management will not advise any requestor on the approval or denial of a data request, nor will they provide any data in response to a FOIA request without the prior approval and direction of the NIJ NamUs Program Manager.

All FOIA requests pertaining to NamUs data should be submitted to the OJP FOIA Office in the Office of the General Counsel. All written FOIA requests should be submitted to the following address:

Office of Justice Programs  
Office of the General Counsel  
810 7<sup>th</sup> St., N.W.  
Washington, D.C. 20531

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

FOIA requests may also be submitted through e-mail to [FOIAOJP@usdoj.gov](mailto:FOIAOJP@usdoj.gov), by fax to 202-307-1419 or via telephone at 202-307-6235.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 8.00 NamUs Staff

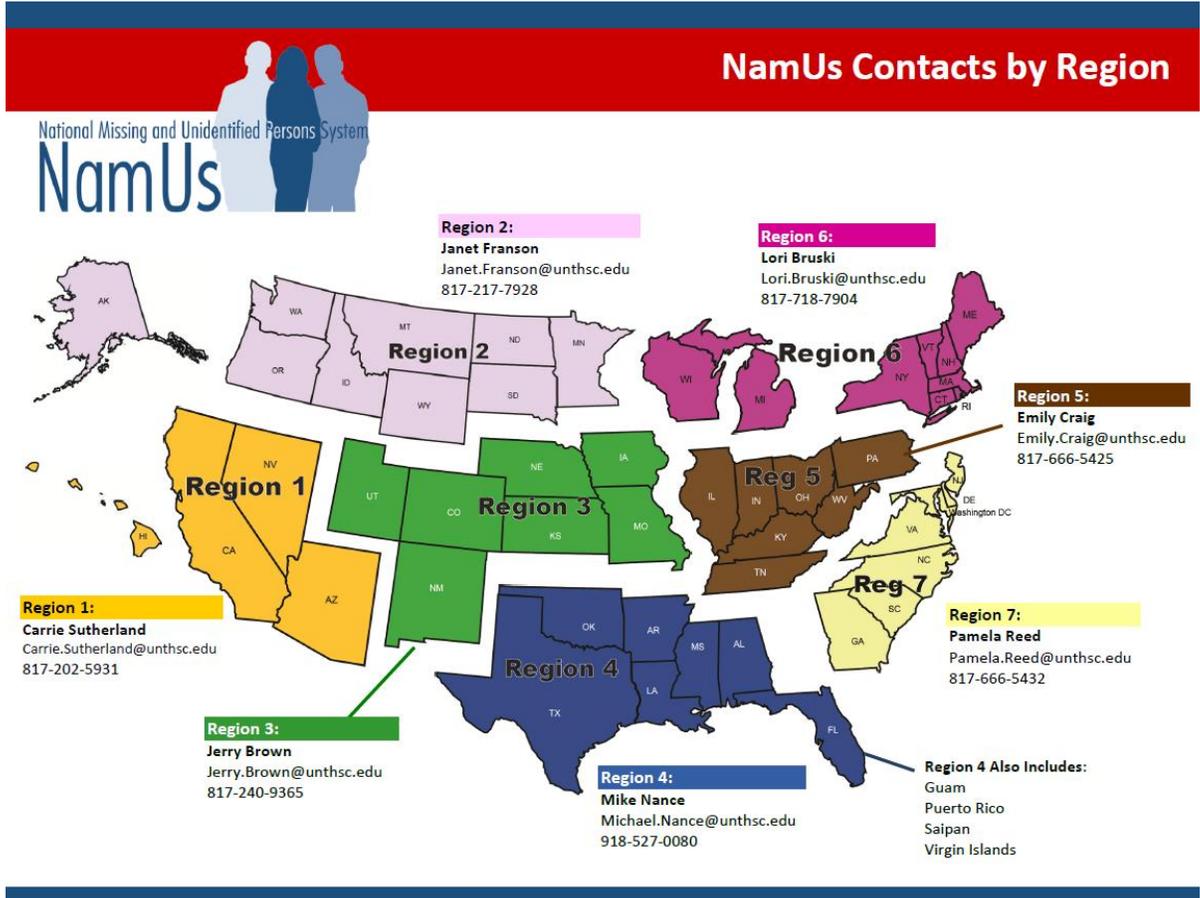
#### 8.01 Personnel Contact List

Name	Area	Position	Phone #1	Phone #2	Email
George Adams	Nationwide	Director, Operations Division	817-735-5451	817-682-7318	<a href="mailto:G.W.Adams@unthsc.edu">G.W.Adams@unthsc.edu</a>
Bill Bailey	Nationwide	Fingerprint Examiner	817-735-5117	817-888-6283	<a href="mailto:William.Bailey@unthsc.edu">William.Bailey@unthsc.edu</a>
Jerry Brown	Region 3	Regional System Administrator	N/A	817-240-9365	<a href="mailto:Jerry.Brown@unthsc.edu">Jerry.Brown@unthsc.edu</a>
Lori Bruski	Region 6	Regional System Administrator	N/A	817-718-7904	<a href="mailto:Lori.Bruski@unthsc.edu">Lori.Bruski@unthsc.edu</a>
Emily Craig	Region 5	Regional System Administrator	N/A	817-666-5425	<a href="mailto:Emily.Craig@unthsc.edu">Emily.Craig@unthsc.edu</a>
Darrell Dean	Nationwide	Evidence Custodian / Field Support	817-735-2547	N/A	<a href="mailto:Darrell.Dean@unthsc.edu">Darrell.Dean@unthsc.edu</a>
Dustin Driscoll	Nationwide	NamUs Analyst	N/A	817-240-4106	<a href="mailto:Dustin.Driscoll@unthsc.edu">Dustin.Driscoll@unthsc.edu</a>
Arthur Eisenberg	N/A	Director, Dept. of Forensic & Inv. Genetics	817-735-0555	817-228-5988	<a href="mailto:Arthur.Eisenberg@unthsc.edu">Arthur.Eisenberg@unthsc.edu</a>
John Filippi	N/A	Forensic Odontologist	N/A	817-666-5424	<a href="mailto:John.Filippi@unthsc.edu">John.Filippi@unthsc.edu</a>
Janet Franson	Region 2	Regional System Administrator	406-323-2273	817-217-7928	<a href="mailto:Janet.Franson@unthsc.edu">Janet.Franson@unthsc.edu</a>
Clyde Knight	Nationwide	Regional System Administrator	817-735-5476	682-201-6186	<a href="mailto:Clyde.Knight@unthsc.edu">Clyde.Knight@unthsc.edu</a>
Todd Matthews	Nationwide	Communications Manager	N/A	817-408-6723	<a href="mailto:J.Todd.Matthews@unthsc.edu">J.Todd.Matthews@unthsc.edu</a>
Mike Nance	Region 4	Regional System Administrator	N/A	918-527-0080	<a href="mailto:Michael.Nance@unthsc.edu">Michael.Nance@unthsc.edu</a>
Pamela Reed	Region 7	Regional System Administrator	N/A	817-666-5432	<a href="mailto:Pamela.Reed@unthsc.edu">Pamela.Reed@unthsc.edu</a>
Ruth Rodriguez-Dunnahoo	Nationwide	NamUs Administrative Specialist	817-735-5010	N/A	<a href="mailto:Ruth.Rodriguez-Dunnahoo@unthsc.edu">Ruth.Rodriguez-Dunnahoo@unthsc.edu</a>
Rich Scanlon	N/A	Forensic Odontologist	N/A	817-487-9645	<a href="mailto:Richard.Scanlon@unthsc.edu">Richard.Scanlon@unthsc.edu</a>
B.J. Spamer	Nationwide	Director, Training & Analysis Div.	817-735-5473	817-964-1879	<a href="mailto:BJ.Spamer@unthsc.edu">BJ.Spamer@unthsc.edu</a>
Sue Stiltner	Nationwide	NamUs ViCAP Liaison	703-632-4173	817-487-9970	<a href="mailto:Suzanne.Stiltner@unthsc.edu">Suzanne.Stiltner@unthsc.edu</a>
Carrie Sutherland	Region 1	Regional System Administrator	N/A	817-202-5931	<a href="mailto:Carrie.Sutherland@unthsc.edu">Carrie.Sutherland@unthsc.edu</a>

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

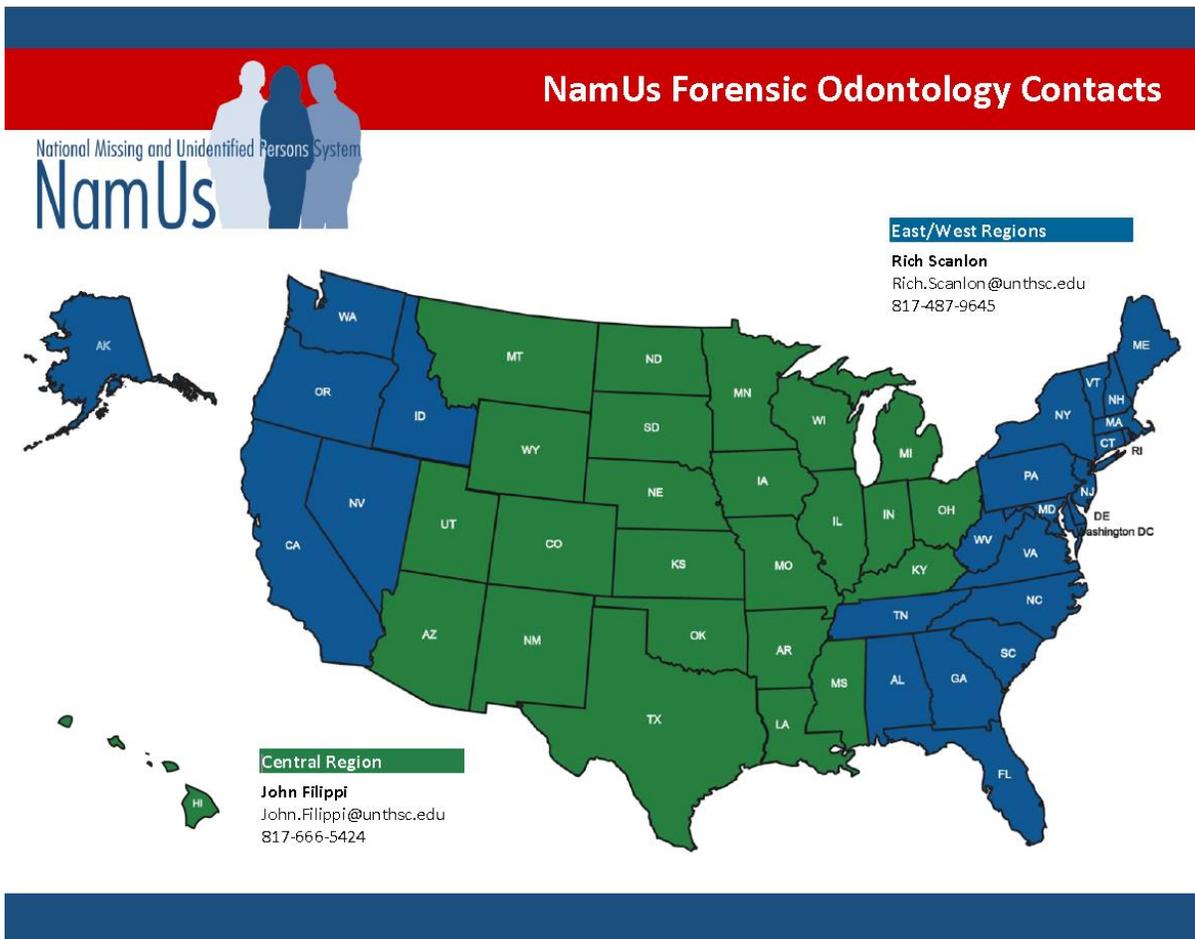
### 8.02 NamUs Regional System Administrator Assignment Map



# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 8.03 NamUs Forensic Odontologist Assignment Map



# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 9.00 Regional System Administrator Responsibilities

#### 9.01 The Role of the RSA

The role of the NamUs RSA is to assist family members of missing persons and criminal justice agencies across the United States with missing and unidentified person cases. RSAs help agencies provide the most accurate information possible and secure forensic resources where needed. CJAs will determine what information is appropriate for public view in their particular case. However, the NamUs RSA will also vet case information for appropriateness of public dissemination per the NamUs Policy Manual and will work with CJAs to resolve any conflicts between what the agency wishes to publicize and NamUs policies. Information may also be excluded from NamUs databases or made not viewable to the public at the discretion of the RSA or NamUs management when it is deemed inappropriate for entry and/or public view. Prior to a case being published for public viewing, the RSA shall contact the CJA of record and secure that agency's permission to publish. If NamUs personnel – Directors, RSAs, ViCAP Analyst, etc. – have documented an agency's permission to publish in the activity log, a second call to the agency is not required. However, RSAs are encouraged to develop relationships with all agencies and users assigned to their geographic region.

With the exception of Public Users, the RSA will vet each new user registration to ensure that all users meet the criteria to view and edit LES/CJI per the NamUs Policy Manual.

An RSA does not accept physical evidence from any Public User, such as fingerprint cards, dental radiographs or DNA profiles to be uploaded or compared in CODIS. The public user will be instructed to release such items to the CJA of record, or the appropriate forensic specialist working in conjunction with the CJA to maintain the integrity of the chain of custody.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 10.00 General User Registration Issues

#### 10.01 Terms of Use

All users who wish to register for NamUs MP/UP/UPC must personally register and agree to the NamUs Terms of Use and Privacy Policy. Users may not register by proxy through another party.

All parties must agree to the NamUs Terms of Use and Privacy Policy at the time of registration. No generic and/or shared user profiles are permitted (e.g., “Coroner Investigator”). No user is permitted to access the NamUs MP/UP/UCP databases using another registered user’s credentials. No user may attempt to use permissions above those granted by his/her vetted and approved user profile. Violations are considered a serious security breach and may result in removal of the user from NamUs by disabling his/her account.

#### 10.02 User Approval

No Regional System Administrator (RSA) or other NamUs staff member may approve a user registration if it contains a known alias name, fictitious name or group/agency name in the first, middle and/or last name fields of the user profile. With the exception of legal name changes – such as a legal name change due to marriage – no user’s first, middle and/or last name may be overwritten in the user profile. Overwriting a user’s first, middle and/or last name is considered a security violation which may result in removal of the user from NamUs and/or termination of NamUs personnel involved in the incident. Requests to change a user’s first, middle and/or last name due to legal name change must be routed through NamUs Senior Management.

#### 10.03 Required Information

Before a user may be approved and activated by an RSA to use the NamUs MP/UP/UCP databases, the RSA must review the information contained in the user profile for completeness and accuracy, in accordance with current NamUs policies and procedures. Upon a user’s request for renewal, or when an account comes to the attention of the RSA for any other reason, the user profile will be reviewed again to ensure that it complies with current NamUs policies and procedures. Any missing information or issues with the user profile will be addressed by the RSA at that time by contacting the user and/or sponsor as needed. Any new information, such as a change in employment or role within a criminal justice agency, must be verified before the RSA may approve a user’s renewal request. Information must be appropriate for the field in which the information was entered.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 10.04 User Roles and General Vetting Issues

Registered users of NamUs can access and/or edit varying levels of information based on their role and the permissions granted in the system. All users are required to register for a specific role within NamUs and with the exception of Public Users, all users are vetted prior to activation in the system. When public users are found to have provided false or inappropriate information, the public user may be removed from the system. Registrants providing generic or alias user names (e.g., Forensic Investigator) will not be granted access to NamUs.

Non-U.S. citizens and non-U.S. criminal justice agencies do not qualify to register for access to NamUs at this time; however, non-U.S. users may search the NamUs databases without registering, to view non-LES/CJI information that is available to the general public. Information related to a foreign criminal justice agency may be added to the "Police" screen or the "Circumstances" screen if a foreign agency is involved in the investigation.

After each new CJA is vetted, approved and activated, he or she must adhere to the policies and protocols of their sponsoring CJA when accessing or interacting with NamUs. The sponsoring agency is responsible for the conduct of the users they have sponsored or authorized for NamUs access. Any user editing information outside his or her permission levels, or in violation of his or her agency's policies and/or protocols, may have access to NamUs suspended. Any user providing false information may have his or her access to NamUs suspended.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 11.00 User Permission Levels – MP/UP/UCP Databases

#### 11.01 Criminal Justice Agency Users and Permissions

It shall be the responsibility of the RSA to confirm that a user's agency meets the criteria of a CJA, as defined in the Glossary section of the NamUs Policy Manual. A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included<sup>3</sup>. Military Criminal Justice users are included in the CJA definition as long as they are associated with a criminal investigative division or a forensic medical/pathology unit of the United States Military.

CJA users shall be granted Full View and Limited Edit permissions in the MP/UP/UCP databases. Criminal justice users include the following user categories:

- CJA Administrator
- Law Enforcement
- Medical Examiner(ME)/Coroner
- Medicolegal Death Investigator
- Forensic Anthropology/Pathology

Full View allows users to view all cases that are published, along with any unpublished cases to which they are assigned as a Local Contact, Case Manager or "Entered By" party. Limited Edit allows these users to edit all fields within a case to which they are assigned as a Local Contact, Case Manager or "Entered By" party. Limited Edit does not allow users to edit cases for which they are not specifically associated.

Under this policy, CJA users include only users who are paid employees of a criminal justice agency or are volunteer personnel with a credentialing letter on file with NamUs. For guidelines related to non-paid users, see NamUs Operations Manual policy number 4.02 titled "NamUs MP/UP/UPC - Volunteers".

---

<sup>3</sup> Criminal Justice Information Security Policy Version 5.0 February 9, 2011, Item 3.2.4

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### **11.02 Forensic Anthropology/Pathology Users**

Forensic Anthropology/Pathology Users will have the same permissions as those of a CJA user for the geographic area in which they are activated. The Forensic Anthropology/Pathology user is required to be sponsored by a CJA with jurisdictional authority. Forensic Anthropology/Pathology users will have no field restrictions as most function as the de facto medical examiner or coroner.

#### **11.03 Military/Federal Criminal Justice Users**

Military/Federal Criminal Justice users will be activated in all states and territories of the United States as Law Enforcement users or Medical Examiner/Coroner users, as appropriate, with Full View and Limited Edit privileges.

#### **11.04 Specialized CJA Users: Forensic Subject Matter Experts**

Depending upon their roles and authorization to enter/edit cases on behalf of Case Owners, forensic subject matter experts may be validated and activated under any of the CJA categories listed in Section 10.01 of this NamUs Policy Manual, or they may be validated and activated under one of the following specialized forensic user categories which are granted Full View and restricted Limited Edit:

- Forensic Odontologist
- Fingerprint Examiner
- DNA Specialist

The DNA Specialist is required to be an active CODIS Administrator, Analyst or other DNA subject matter expert employed by a public CODIS laboratory.

These user categories are granted Full View, but have a restricted Limited Edit permission which allows them to only edit the fields relevant to their forensic disciplines/areas of expertise. Forensic Odontologists can only edit fields in the “Dental” screen, Fingerprint Examiners can only edit fields in the “Fingerprints” screen and DNA Specialists can only edit fields in the “DNA” screen. Unlike Law Enforcement and other CJA categories noted above, these specialized forensic user categories allow users to edit all cases within the geographic areas in which they are activated, regardless of whether they are assigned to the case as a Local Contact or Case Manager contact.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

Users in these disciplines who have been granted authorization to edit additional data by the Case Owners should be classified as Law Enforcement, Medicolegal Death Investigators or another appropriate CJA category for unrestricted Limited Edit access.

#### **11.05 NamUs Administration/Staff**

The following administrative user categories shall be granted enhanced Full View and Full Edit permissions in the MP/UP/UCP databases. Enhanced Full View allows these users to see all unpublished cases, regardless of the geographic areas in which they are activated.

- Super Administrator
- Regional System Administrator (RSA) – NamUs
- Regional System Administrator (RSA) – NCMEC

#### **11.06 Grandfathered User Categories**

Some of the above user categories described in section 10.00 of the NamUs Policy Manual were added to NamUs after the program's inception. Some existing, previously vetted users will need to be converted to the appropriate user category and permissions as they are located in the normal course of business operations (e.g., user renewal/revalidation process).

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 12.00 Vetting New NamUs User Registrations

Each user who registers for NamUs is automatically assigned a unique record identification number in the NamUs database. The following fields in the user profile are static fields that **MAY NOT BE OVERWRITTEN** by the user, RSA or NamUs management/administrators:

- First Name
- Middle Name
- Last Name

The only exception to the above policy is in regard to a legal name change, such as a name change associated with marriage. In case of a legal name change, the RSA shall notify NamUs Senior Management, who will update the user profile after verifying the name change with appropriate documentation.

Any name changes not approved by NamUs Senior Management will be considered a breach of security in attempting to circumvent the vetting/re-validation process of users. All users must register with the NamUs MP/UP/UCP database(s) under the appropriate user categories, as described in Section A of this policy.

The NamUs RSA will validate that the contact information entered by the user is accurate. If the user provides a public email address in his/her user profile (e.g., Gmail or Yahoo), the RSA is required to call the agency's general communications line to validate the user's information.

The NamUs RSA will call or email the sponsor indicated by the user to validate the user as a CJA employee, or to obtain a sponsorship/credentialing letter from the appropriate CJA for law enforcement volunteers (see NamUs Operations Manual policy number 4.08 titled "NamUs MP/UP/UPC - Volunteers"). If the sponsor does not respond in a timely manner, or the NamUs RSA questions the appropriateness of the listed sponsor, the NamUs RSA shall independently contact administrative offices, unit commanders, or other personnel deemed appropriate to verify the employment of the registering user.

The NamUs RSA shall note the following in the "Verified By" textbox within the user's profile:

- All parties contacted for verification, including contact information (email/phone).
- The date and time of contact/validation.
- The RSA's first and last name (not initials).

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

- A written statement summarizing the sponsor's verification (e.g., SAC Jones confirmed that SA Smith is employed within the FBI ViCAP Unit).
- No written letter of authorization is required from the Criminal Justice Agency verifying the user for their paid employees.
- Criminal Justice Agencies will be required to furnish a letter (on agency letterhead) credentialing volunteers.

The NamUs RSA is not in a position to judge the qualifications of criminal justice users or direct agencies in the use of their personnel. Each agency may have different criteria – or no criteria at all – related to the agency's personnel. Many odontologists, anthropologists and other forensic experts function in multiple capacities. The forensic specialists may provide analysis and also serve as the investigator on the case. The role of the MP/UP user will be defined by agency policies and administrative practices, and not by the RSA. Should there be a complaint that the agency's internal policies and practices have been violated by the user, and the complaint is confirmed upon inquiry by the RSA, the Director may suspend the user's access to the NamUs MP/UP/UCP database in full or in part.

NCMEC RSAs will not have the ability to vet users. NCMEC RSAs will defer to the appropriate NamUs RSAs or management to validate users.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 13.00 MP/UP/UCP User Renewals

#### 13.01 User Renewal Cycles

MP/UP/UCP user registrations are active for one year after appropriate verification of the user's information by the NamUs Regional System Administrator (RSA), in accordance with current NamUs policies and procedures. Thirty days from the date of an MP/UP/UCP user's account expiration, a system-generated email is sent to the user, notifying him/her of the user expiration and providing instructions for the user to request renewal of his/her NamUs account. The user will also see the number of days remaining before his/her account expires on the MP/UP/UCP database home page each time the user logs into the applicable NamUs database. It is the responsibility of the user to request renewal of his/her MP/UP/UCP user account by following the instructions provided in the system-generated email and/or NamUs website; however, the NamUs RSAs may proactively review their lists of expired users and attempt contact to renew users who may have allowed their accounts to expire. The NamUs Training and Analysis Division can assist RSAs in developing spreadsheets of expired users – to include email addresses and telephone numbers – to assist with this process.

#### 13.02 Responding to Renewal Requests

When a request for account renewal is sent, the RSA will receive a system-generated email which provides the user's information. Upon receipt of this notification, it is the responsibility of the RSA to review the user's profile for accuracy/completeness and contact the user's sponsor to confirm that the user is still employed with the agency, in a capacity that requires him/her to continue having access to the NamUs MP/UP/UCP databases. This contact may be made via telephone, email or fax. If after attempting to contact a sponsor or user via email to no avail, the RSA should attempt to contact the individual directly via telephone. The RSA may also attempt to contact the individual through the agency's general telephone number, in the event that direct extensions listed on the user's profile have changed. Often, agencies' Internet firewalls may block incoming emails, making telephone follow-up necessary to ensure the highest level of customer service to NamUs users. If a user has provided a non-government/non-agency email address for his/her sponsor (e.g., Yahoo or Gmail account), the sponsor's agency must be contacted by telephone to validate they are with a criminal justice agency or other appropriate agency to sponsor the user.

After receiving authorization from the sponsor to renew the user's account in the NamUs MP/UP/UCP databases, the RSA shall document in the "Verified By" box on the user's profile all efforts that were taken to re-validate the user's account for renewal, in accordance with the

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

NamUs Operations Manual procedure titled “Vetting Users”. The RSA should then review the user’s activated counties to ensure they are still appropriate to the user and click the “Renew Now” link on the user’s profile to renew the user’s MP/UP/UCP account for another year.

#### **13.03 Users No Longer Sponsored for Access to NamUs Databases**

During the process of responding to new user registrations and requests for user renewals, it is sometimes discovered that a user who was associated with a case in NamUs (e.g., entering party or Case Manager) is no longer employed by the investigating agency or has moved into a different role within the agency (e.g., detective reassigned from missing persons to fugitive recovery). Users with CJA access to NamUs who are no longer employed with the CJA will have their accounts “Disabled” or changed to a “Public User” access level; these users will never be deleted from the system or have their accounts reused by changing the name to a new investigator from the CJA, as these actions will impact case contacts, case chronology logs and other system audits. The RSA should determine the point of contact at the appropriate CJA who will serve as the new Case Manager and/or Local Contact for all cases previously assigned to the Disabled user. If that individual is not currently registered for NamUs, the RSA should assist the user with registration and facilitate the transfer of all applicable cases to that new contact by manually placing the individual into the Case Manager and/or Local Contact fields, or requesting this process be automated through the UNT Health Science Center Information Technology Services Division. Should a new user with the appropriate CJA decline to become the new Case Manager and/or Local Contact for an existing case, the RSA will assume the Case Manager role until a new Case Manager can be located and assigned.

#### **13.04 Revalidation/Renewal of User Account**

Each user account will expire one year from the original date of registration/activation, unless renewed by the NamUs RSA. It is the responsibility of the NamUs user to request renewal of his/her NamUs user account(s) for the MP/UP/UCP databases. When a user requests renewal of his/her user account(s), an automatic notification will be emailed to the appropriate RSA for review and handling. Upon notification of a user’s request for the renewal of an MP/UP/UCP user account, the RSA shall:

- Call or email the sponsor indicated by the user to re-validate the user as a CJA employee, or obtain an updated sponsorship/credentialing letter from the appropriate CJA for law enforcement volunteers (see NamUs Operations Manual policy number 4.08 titled “NamUs MP/UP/UPC - Volunteers). If the sponsor does not respond in a timely manner, or the NamUs RSA questions the appropriateness of the listed sponsor, the

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

NamUs RSA shall independently contact administrative offices, unit commanders, or other personnel deemed appropriate to verify the employment of the registering user.

- Note the following in the “Verified By” textbox within the user’s profile:
  - All parties contacted for verification, including contact information (email/phone).
  - The date and time of contact/validation.
  - The RSA’s first and last name (not initials).
  - A written statement summarizing the sponsor’s verification (e.g., SAC Jones confirmed that SA Smith is employed within the FBI ViCAP Unit).
  - No written letter of authorization is required from the Criminal Justice Agency verifying the user for their paid employees.
  - Criminal Justice Agencies will be required to furnish a letter (on agency letterhead) credentialing volunteers.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 14.00 Case Owners/Managers

#### 14.01 Roles and Responsibilities

Every MP/UP/UCP case will have only one Case Owner. The Case Owner will be assigned as a Case Manager contact to the case and will control the addition, alteration or deletion of any additional Local Contacts or Case Manager contacts on the case in conjunction with the NamUs RSA. The RSA will make changes to the NamUs Contact screen only at the direction of the Case Owner.

The NamUs MP/UP/UCP Case Owner will be a representative of a criminal justice agency (CJA) that has jurisdiction over the case. The case owner must be a registered, vetted NamUs user. Should there be a dispute between two CJAs claiming joint jurisdiction over a case, the Regional System Administrator (RSA) may make a determination of the Case Owner based on the agency of record (ORI) in NCIC. Should an NCIC record not exist, or multiple NCIC records exist, the RSA shall use his or her discretion in determining the appropriate Case Owner or defer to NamUs Senior Management to make the final determination.

With the permission of the original Case Owner, one or more additional Case Manager(s) may be assigned to manage the case. The Case Manager must be a registered, vetted NamUs user associated with a CJA. The Case Manager may be removed at any time at the discretion of the Case Owner or by the RSA if the Case Manager violates the policies of NamUs or acts in a manner not in the best interest of NamUs or the CJA. Any disputes the RSA is not able to resolve should be referred to NamUs Senior Management for resolution.

#### 14.02 Case Owner/Case Manager Permissions

The Case Manager(s) and Case Owner will not have any permissions other than those granted in accordance with their vetted profiles. Case Managers and Case Owners may request to publish or archive cases. No cases may be deleted, with the exception of duplicate cases that can only be deleted by NamUs Senior Management. After review for completeness and appropriateness, the RSA may approve the publication of a case with the permission of any individual who has been authorized by the Case Owner to serve as a Case Manager for that case. No case may be published without the permission of an appropriate Case Manager, and should include documentation by the RSA in the Activity Log of the case.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 15.00 NamUs MP/UP/UCP Volunteer Users

#### 15.01 UNTCHI Forensic Services Unit

At this time UNTCHI-FSU has no volunteer program in place.

#### 15.02 Volunteer Concept/Vetting Process

Volunteers are part of the core mission of NamUs. The real power of volunteer support for law enforcement and NamUs is to harness the volunteer's passion and dedication. NamUs will allow volunteers to register as a law enforcement user for any criminal justice agency (including medical examiners and coroners) under the conditions as follows:

- The agency provides the appropriate NamUs RSA with a credentialing letter on agency letterhead. The RSA will forward a scanned copy to the National Director of Operations.
- The letter must indicate that the volunteer is qualified to see and work with law enforcement sensitive and/or criminal justice information.
- In sponsoring the volunteer, the agency must articulate that the volunteer works under the authority of the agency and/or the agency is responsible for the actions of the volunteer.
- The National Director of Operations will print out a copy and retain in an internal file as a backup to the RSA's copy.
- It is the responsibility of the agency to notify NamUs when the volunteer no longer possesses the privileges and sponsorship of the agency – regardless of whether the letter has a naturally ending expiration date, NamUs must be notified so the civilian's credentials can be placed in an inactive status. Security is paramount and NamUs must ensure that only those that have the right to view sensitive information have that access. Verification of the individual users is designed to identify circumstances where the volunteer is no longer active or an entrusted member of the sponsoring agency.

#### 15.03 Volunteers with Existing Elevated Permissions to UP/MP Databases

When the renewal process occurs or circumstances arise where a public user is acting as a case manager or in another heightened user role, the RSA should advise the public user that it will be necessary to be credentialed by the sponsoring LE agency for which

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

they are supporting. RSAs must remove LES viewing/editing privileges from public users with LE view access until the credentialing process is completed.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 16.00 Entry, Acceptance and Publication of Cases in NamUs

#### 16.01 Manual Case Entry

Cases may be entered into the NamUs Missing Person (MP) database by any registered user, including Public Users; however, all missing person cases must be validated with an appropriate CJA prior to publication in NamUs. Public Users will be recorded as the “Entered By” party on MP cases they have entered into the system; however, they will no longer have the ability to edit case data once the case has been accepted into the NamUs MP database by the RSA.

Users granted CJA access to the NamUs databases are given “Limited Edit” permission which allows them to enter cases into the NamUs MP/UP/UCP databases and edit cases on which they are assigned as the Case Manager and/or Local Contact. Regional System Administrators and Project Administrators are granted full edit privileges.

Unidentified Person (UP) and Unclaimed Person (UCP) cases may only be entered by registered users who have been properly vetted and granted CJA access (or higher) to the UP/UCP databases. Public Users may not enter cases into the NamUs UP/UCP databases.

Case Managers and Local Contacts are assigned to all NamUs cases by the RSA, at the direction of the Case Owner. Permissions for Local Contact and Case Manager contacts will be in conformance with their vetted user profiles.

#### 16.02 Electronic Data Crosswalk Protocols

CJAs may submit multiple cases to NamUs via upload/crosswalk protocols once the case data has been reviewed by the RSA, who will ensure that all mandatory fields are included in the data, in accordance with current policies/procedures. It will be the duty of the RSA to remain updated on current published policies/procedures.

#### 16.03 Minimum Mandatory Case Data

The minimum required data for RSA acceptance of an **MP case** includes an entry into all of the following fields:

1. First Name
2. Last Name
3. Age
4. Sex

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

5. Race
6. Height
7. DNA Status
8. Dental Status
9. City Missing
10. State Missing
11. Date Last Known Alive (LKA)
12. Circumstance of death – ensure that there is no Personally Identifiable Information (PII) or Law Enforcement Sensitive (LES) information included in the publicly viewable text field
13. Hair Color
14. Eye Color
15. Fingerprint Status
16. Local Contact's Relationship

The minimum required data for RSA acceptance of a **UP case** includes entry into all of the following fields:

1. Case Number or NCIC number
2. Date Found
3. Estimated Age (including "Cannot Determine")
4. Race (including "Unsure")
5. Sex (including "Unsure")
6. Weight (including "Cannot Estimate")
7. Height (including "Cannot Estimate")
8. Body Condition
9. State Found
10. County Found
11. Circumstance of death – ensure that there is no Law Enforcement Sensitive (LES) or Personally Identifiable Information (PII) included in the publicly viewable Circumstances text field
12. Fingerprint availability – select one of three categories
13. Dental availability – select one of three categories
14. DNA availability – select one of five categories

When all mandatory fields are completed in a NamUs MP/UP/UCP case, the case can be submitted to NamUs for the RSA to review, accept and publish if/when the case meets appropriate NamUs MP/UP/UCP standards.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 16.04 “Pending” NamUs Case Statuses

An “Incomplete” case is one in which the minimum mandatory data outlined in section 15.03 of the NamUs Policy Manual has not been entered into the NamUs record. Cases cannot be “Accepted” until this minimum mandatory data is entered.

An “Accepted” case is one in which all NamUs MP/UP/UCP mandatory fields have appropriate entries, including an agency case number, and the RSA has clicked the “Accept” button on the case. NCIC entry is not mandatory to accept a case into NamUs RSAs are encouraged to “accept” a case at the earliest opportunity so that case tracking takes effect; until a case is “accepted”, no changes are tracked in the NamUs databases. Once a case is “Accepted”, a public user will no longer have the ability to edit the case or view fields other than publicly viewable fields.

#### 16.05 Case Publication

A “Published” case is a case that adheres to all current NamUs MP/UP/UCP policies related to public viewing, where the RSA has contacted the Case Owner/Case Manager to secure permission to publish the case for public viewing, and that permission has been documented by the RSA in the case Activity Log. The RSA does not have authority to publish any case without agency approval and documentation of such approval in the Activity Log.

Prior to publication, the RSA shall:

1. Conduct an initial administrative review of all screens for completeness of data and appropriateness of content. Any instances of personally identifiable information (PII), law enforcement sensitive (LES) information and protected Health Insurance Portability Accountability Act (HIPAA) information will be properly addressed by the RSA.
2. Ensure that the case contains an NCIC number, LEA case number, or other identifiable CJA number.
3. If necessary, contact the submitting or investigating agency to obtain any missing information (cases may have been imported with incomplete information).
4. Ensure that the “Local Contact” on the “Case Information” screen is correct.
5. Ensure the “Case Manager” is authorized by the jurisdictional CJA and/or Case Owner to manage the case.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

6. Send an email to the appropriate NamUs Forensic Subject Matter Expert (SME) to review any images and/or coding related to fingerprint or dental information, if present. The NamUs Forensic SME may contact the investigating agency if there are concerns with the biometric data or the SME can offer additional services to the agency.
7. Review all case images with regard to appropriateness for upload to NamUs and potential restriction from public viewing:
  - a. Crime scene photos shall be restricted from public view unless the CJA specifically authorizes the publication of the image **and** the image is not inappropriate for public viewing (see bullet item “7b”) **and** publication of the crime scene image has the potential to assist in the identification of the victim (e.g., crime scene photo is the only image depicting the facial features of an unidentified person because an original case file was lost or destroyed).
  - b. At the discretion of the RSA and NamUs management, images that would offend the senses of an ordinary citizen (e.g., mutilated bodies or images showing exposed genital areas) shall be restricted from public view or removed from NamUs if they have no potential to assist in the identification of the victim, with the consent of the Case Owner/Case Manager.
  - c. Restrictions imposed by the CJA or the CJA’s state statutes – such as the Dale Earnhardt Law in Florida which restricts dissemination of autopsy photographs – will supersede all NamUs policies related to the upload and publication of images.
  - d. If an image is deemed unacceptable for public viewing, the RSA may recommend a facial reconstruction or artist rendering to be added to the NamUs file as a publicly viewable image. The RSA may refer the investigating agency to established resources to obtain free forensic art services. When facial reconstructions or artists renderings are added to NamUs as publicly viewable images, the original image may be retained in the NamUs file – restricted from public view – so that it remains available to appropriately vetted CJA users.
8. Review each document uploaded to the NamUs MP/UP/UCP database to ensure that there is no PII or LES information contained in the documents that will be publicly viewable. The RSA must also ensure that there are no Social Security numbers present on any documents, regardless of whether or not they will be publicly viewable.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

- a. Offense reports, medical reports and reports related to potential associations may be uploaded by agencies but restricted from public viewing, provided they do not contain information protected under HIPAA.
  - b. Some fingerprint and/or dental information may be uploaded to the NamUs “Documents” screen – as opposed to the “Images” screen – as PDF documents. If dental or fingerprint information is present, the RSA shall send an email to the appropriate NamUs Forensic SME to review this biometric data to ensure that the information is transferred to – or duplicated in – the appropriate areas of the NamUs case file (e.g., Dental screen versus Documents), and to contact the agency if it is necessary to obtain better quality images, clarify information, etc. The appropriate SME experts should be used extensively by the RSA to improve the quality of the biometrics in NamUs and to conform to national standards outside the purview of the RSA.
9. Contact the submitting and/or investigating CJA to confirm the accuracy of all case information and obtain authorization prior to publishing the case in NamUs. The RSA will document the authorization to publish in the Activity Log and include the name and contact information of the individual who has given the RSA permission to publish. Many MP/UP/UCP cases involve current criminal investigations and may contain confidential information, or the existence of the case itself may be considered law enforcement sensitive; CJAs may wish to have such cases remain restricted from public view. It is up to the CJA to authorize the publication of the case, not the RSA.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### 17.00 Unverifiable Cases

##### 17.01 Unverifiable MP Cases

A member of the general public who registers for the NamUs MP database as a “Public User” receives an automatic, system-generated password which allows him or her to log into the MP database and enter new cases without being vetted by a NamUs RSA. It is the responsibility of the RSA to verify all Public User entries into the MP database with appropriate criminal justice agencies before proceeding with case acceptance and/or publication.

If the relationship between the missing person and the Public User who has entered the case into the NamUs MP database is not noted, or is unclear from the data entered into NamUs, the RSA should first make an effort to clarify the relationship. Cases may be entered by “concerned citizens” who have no relationship to a missing person, or they may be entered by friends, family members or others who had a personal relationship with the missing person prior to his or her disappearance. Cases entered by individuals with a purported personal relationship to the missing person may require additional technical assistance from the RSA when cases cannot immediately be validated.

**For all cases entered into the NamUs MP database by Public Users, the RSA will:**

- Review any circumstances and/or additional data in the case to ensure that the Public User has entered a case that purports to involve a missing person, defined as *an individual whose disappearance is possibly not voluntary and whose whereabouts are unknown to criminal justice agencies and/or family members.*

If there is clear indication that the case does not involve a missing person, as defined above, and/or there is suspicion that the user has intentionally or unintentionally misused the NamUs system, the RSA will contact the Public User to explain the role of NamUs and determine if there are additional facts or circumstances that would assist in validating the case. The RSA will use his or her discretion in providing any additional advice or technical support that is deemed appropriate.

If after additional contact with the Public User the RSA determines that the case does not involve a missing person, as defined above, the RSA will deem the case “Unverifiable” and will add an Activity Log entry documenting his or her efforts to validate the case and why the case is unverifiable. The case can then be removed from the RSA’s pending case queue and transferred to the “Unverifiable” case queue.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**If a review of the case details and/or additional information from the Public User indicates that the case *does* potentially involve a missing person, the RSA will:**

- Review the Public User's entry to determine if a jurisdictional criminal justice agency has been entered into the case or can be determined from the data entered by the Public User (e.g., city and state missing).
- Contact the appropriate jurisdictional agency/agencies via telephone or email to determine if a missing person report is already on file with the agency.
- If a report is already on file with a criminal justice agency, update the NamUs case file with the appropriate agency name, investigator, contact information, case number and/or any additional information provided by the agency. Follow established policies and procedures regarding additional review and publication of the case, where appropriate.

If a report is not already on file, the following additional step will be taken:

- Make an entry into the Activity Log to document the date of the initial RSA review, along with any additional information related to verification attempts (e.g., "Initial review of MP case entered by Public User completed on this date. No LEA noted in case file Left message w/ Det. Smith of Kansas City PD Missing Persons Unit – 555-555-1212 – to determine if a MP report is on file with jurisdictional agency").

**If no missing person report can be located with a criminal justice agency and the NamUs MP case was entered by a Public User with no relationship to the missing person, the RSA shall:**

- Advise the Public User that the case could not be validated and will be archived in the NamUs MP database unless/until the Public User can provide an investigating agency case number and/or additional information from an appropriate criminal justice agency to validate the case.
- Use his or her discretion to request searches from the NamUs Analyst or conduct additional searches of news articles, missing person websites, etc. in an attempt to locate additional information to validate the case.
- Make a notation in the Activity Log to document case validation efforts and any applicable correspondence with the Public User (e.g., "No missing person report could be located with the Denver Police Department or Colorado MP Clearinghouse. Entering party was notified that case could not be validated and will be archived unless the

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

entering party provides an investigating agency and case number, or additional information to validate the case”).

**If no missing person report can be located with a criminal justice agency and the NamUs MP case was entered by a Public User who indicates that he or she is a family member, friend or associate of the missing person, the RSA shall:**

- Explain to the Public User that a case must be validated with a criminal justice agency prior to acceptance and publication in the NamUs MP database.
- As needed, provide the Public User with guidance on reporting a missing person case, to include contact information for the criminal justice agency/agencies in the appropriate jurisdiction from which the individual was reported missing.
- Provide additional technical support and assistance to the Public User, as needed, to have a missing person report filed, or obtain additional information required to validate the case in NamUs. The RSA may use his or her discretion to contact criminal justice agencies on behalf of the reporting party to provide additional support, and should make reasonable efforts to assist friends, family members, and associates of missing persons prior to deeming a case “Unverifiable”.
- Use his or her discretion to request searches from the NamUs Analyst or conduct additional searches of news articles, missing person websites, etc. in an attempt to locate additional information to validate the case.
- Make a notation in the Activity Log to document case validation efforts and any applicable correspondence with the Public User (e.g., “The entering party, MP’s mother, was notified that a report to law enforcement is required for validation and potential publication. Mother was provided contact information for Fort Worth PD on this date to file a report.”).
- If/when a report is filed with a criminal justice agency, follow established protocols to have the case information reviewed by the investigating agency and to have the case published, where appropriate.

**Following all of the applicable protocols noted above, if the RSA is still unable to validate a case entered by a Public User for acceptance into NamUs:**

- After a period of no less than 60 days from the RSA’s initial review of the case, as documented in the Activity Log, the RSA may deem the case unverifiable and move the

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

case to the “Unverifiable” case queue. The RSA may use his or her discretion to maintain the case in the “Pending” queue for longer than 90 days if he or she is continuing to assist the entering party with a report to law enforcement or is providing additional technical assistance.

- The RSA will document final efforts to validate the case in the Activity Log, along with the reason for archival as an “unverifiable” case and any additional technical assistance or instruction provided to the entering party.
- An “Unverifiable” case may be returned to the “Pending” or published queue at any time, in the event that the circumstances of the case change (e.g., family is later successful in filing a missing person report).

#### **17.02 Unverifiable UP Cases:**

Currently there is no unverifiable case category in the NamUs UP database.

#### **17.03 Unverifiable UCP Cases:**

Currently there is no unverifiable case category in NamUs UCP database.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 18.00 NCMEC Case Selection Criteria

#### 18.01 Assignment of MP Cases to National Center for Missing and Exploited Children (NCMEC)

All missing person (MP) cases entered into NamUs are automatically assigned to an appropriate NamUs or NCMEC RSA based on the information entered into the “Date of Birth” and “Date Last Seen” fields. When these fields are populated, the system automatically calculates the age of the MP at the time of disappearance. If an individual was 17 years or younger at the time of disappearance, the case is automatically assigned to the appropriate NCMEC RSA for the geographic region in which the MP was last seen alive. If an individual was 18 years or older at the time of disappearance, the case is automatically assigned to the appropriate NamUs RSA for the geographic region in which the MP was last seen alive.

In some instances, NCMEC may provide assistance to agencies investigating the disappearance of individuals who were 18 to 20 years of age at the time of disappearance under Section 5779 of 42 U.S.C. In these cases, NCMEC RSAs may be manually assigned as the “Regional System Administrator” with the approval of the investigating agency in accordance with the following guidelines:

- NCMEC should make a written request via email to the assigned NamUs RSA to have the case reassigned to a NCMEC RSA.
- All cases involving missing persons between the age of 18 and 20 will first be reviewed by NamUs RSAs, who will verify that the Case Owner/Case Manager from the investigating agency desires NCMEC be added to the case as a “Regional Administrator”.
- The NamUs RSA will facilitate reassignment of the case in NamUs to the appropriate NCMEC RSA once approval is obtained from the Case Owner/Case Manager from the investigating agency.

NCMEC or the investigating agency may decide at any time to refer the “Regional Administrator” responsibilities for a particular MP case back to a NamUs RSA. All such requests should be submitted to the appropriate NamUs RSA for the region in which the MP was last seen alive, who will facilitate the reassignment of the MP case in NamUs.

NCMEC RSAs will assume responsibility for completing the following tasks related to MP cases for which they are assigned as RSAs:

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

- Reviewing all new “Incomplete” MP cases and making contact with the submitting individuals/agencies to complete case data and/or address duplicate entries, where appropriate, in accordance with NamUs/NCMEC policies and procedures.
- Reviewing all “New” and “Accepted” MP cases for validity and completeness/appropriateness of all case information in accordance with NamUs/NCMEC policies and procedures.
- Publishing all “New” and “Accepted” MP cases at the direction of the Case Owner/Case Manager from the appropriate investigating agency and in accordance with NamUs/NCMEC policies and procedures.
- Approving, denying or holding all changes to MP cases.

#### **18.02 Reassignment of MP Cases Not Publishable by NCMEC**

All MP cases assigned to NCMEC shall be reviewed by NCMEC within **30** days of assignment. During that timeframe, the case shall be published by NCMEC or a notation should be made in the Activity Log that an attempt has been made to intake the case at NCMEC and/or publish the case in NamUs. If NCMEC is unable to publish a case due to the lack of an NCIC entry, law enforcement declining NCMEC assistance, inability to validate the case, or some other factor within **60** days from the date of assignment, NCMEC shall notify the appropriate NamUs RSA, who will facilitate the transfer of that case to the NamUs RSA for further review, regardless of the age of the missing person. The NamUs RSA will then take appropriate actions to determine if the case meets the criteria to be published by the NamUs RSA under section 16.05 (Case Publication) of this policy, or be deemed “Unverifiable” under section 17.00 (Unverifiable Cases) of this policy.

NamUs management may review pending cases assigned to NCMEC on a periodic basis and if a case remains unpublished after **90** days without documentation in the NamUs Activity Log that efforts are being made by NCMEC to publish the case, NamUs management may reassign the case to the appropriate NamUs RSA at any time for further action.

#### **18.03 Assignment of UP Cases to NCMEC RSAs**

All UP cases entered into NamUs are automatically assigned to the appropriate NamUs Regional System Administrator (RSA) for the geographic area in which the remains were recovered, which is determined by the “County” and “State” entered into the “Circumstances” screen. NCMEC personnel may be manually assigned as the “Case Manager” for UP cases that potentially

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

involve a juvenile with the approval of the investigating agency, in accordance with the following guidelines:

- NCMEC personnel may be added as the “Case Manager” to UP cases in which the minimum estimated age of the decedent is 17 years or younger, and the maximum estimated age of the decedent is 25 years or younger. NCMEC should make a written request via email to the assigned NamUs RSA to have the case reassigned to a NCMEC staff member.
- All UP cases will first be reviewed by NamUs RSAs, who will verify that the Case Owner/Case Manager from the investigating agency desires NCMEC be added to the case as a “Case Manager”.
- The NamUs RSA will facilitate reassignment of the case in NamUs to the appropriate NCMEC Case Manager once approval is obtained from the Case Owner/Case Manager from the investigating agency.

All potential juvenile UP cases for which NCMEC has not requested assignment as a Case Manager, or the Case Owner/Case Manager from the appropriate investigating agency has declined NCMEC assistance, will remain assigned to the NamUs RSA assigned to the region in which the decedent was located. NCMEC Case Managers will assume responsibility for completing the following tasks related to UP cases for which they are assigned as Case Managers:

- Reviewing all new “Incomplete” UP cases and making contact with the submitting agencies to complete case data and/or address duplicate entries, where appropriate.
- Reviewing all “New” and “Accepted” UP cases for completeness and appropriateness of all case information.
- Publishing all “New”, “Accepted” and “Pending ME/C Approval” cases at the direction of the Case Owner/Case Manager from the appropriate investigating agency.
- Approving, denying or holding all changes.

NCMEC or the investigating agency may decide at any time to refer the “Case Manager” responsibilities for a particular UP case back to a NamUs RSA. All such requests should be submitted to the appropriate NamUs RSA for the region in which the decedent was located, who will facilitate the reassignment of the UP case in NamUs.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

#### **18.04**      **Assignment of UCP Cases to NCMEC RSAs**

NCMEC RSAs and/or Case Managers will not have any responsibilities related to cases entered into the NamUs UCP database.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### 19.00 NEIM / XML Exchanges

To be added later

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

### Glossary

**Accepted Case:** A case is deemed accepted when all mandatory NamUs fields have been completed, the case has been submitted to NamUs, and the RSA has accepted the case into NamUs. Until a case is accepted into the NamUs database, changes are not tracked in the chronology log.

**AFIS:** The Automated Fingerprint Identification System (AFIS) is a database that uses digital imaging technology to capture, store, and analyze fingerprint data. Also see IAFIS.

**Allele:** An alternative form of a gene (one member of a pair) that is located at a specific position on a specific chromosome.

**Anthropologist:** A person who specializes in the science that deals with the origins, physical and cultural development, biological characteristics, and social customs and beliefs of humankind.

**Anatomical Position:** The position with the body erect with the arms at the sides and the palms forward.

**Alien Registration Number (ARN):** An ARN – also referred to as an A-number, A#, Alien Number, Green Card Number – is an identifying number that U.S. Citizenship and Immigration Services (USCIS) assigns to certain aliens, such as those who apply for adjustment of status. A-numbers may consist of 8 or 9 digits. The A-number is assigned to an individual for life, much like a social security number. Alien registration began in August 1940 as a program to record every non-citizen within the United States. The original Act of 1940 was a national security measure, and directed the former INS to fingerprint and register every alien age 14 and older within and entering the United States.

**Autosomal DNA:** Any non–sex-determining chromosome.

**Biometric Data:** Data derived from one or more intrinsic physical traits of humans, typically for the purpose of uniquely identifying individuals from within a population. Biometric data includes – but is not limited to – DNA, fingerprints, palm prints, iris scans, and facial recognition data. Biometric data is considered Criminal Justice Information (CJI).

**BSC:** The Biometric Support Center is a contract agency for the Department of Homeland Security which specializes in the storage, searching and comparison of fingerprint data.

**Case/Incident History:** Information about the specific history of criminal incidents (includes missing persons) – considered part of Criminal Justice Information.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**Case Entry:** Refers to the initial process of entering a case into NamUs. Any registered user can enter a case into the NamUs Missing Person (MP) database. Cases can only be entered into the NamUs Unidentified Person (UP) database by personnel of a CJA or their designees.

**Clearinghouse:** is a physical or electronic office which is a central repository of information on missing persons and or unidentified decedents.

**Criminal Justice Agency (CJA):** A CJA is defined as a U.S. court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included. Military Criminal Justice users are included in the CJA definition as long as they are associated with a criminal investigative division or a forensic medical/pathology unit of the United States Military.

**Criminal Justice Information:** Information necessary for criminal justice agencies to perform their missions. CJI includes – but is not limited to – biometric data, identity history data, biographic data, property data, and case/incident history data.

**Criminal Justice Users:** U.S. users of NamUs who have been vetted as Military/Federal Criminal Justice, Local/State Criminal Justice, Medicolegal/Forensic Specialist, Medical Examiner, Coroner or DNA Specialists.

**Dale Earnhardt Law:** A Florida law which makes autopsy photographs, video and audio recordings confidential. Other states may be passing similar laws.

**DEA:** Drug Enforcement Administration.

**DHS:** Department of Homeland Security.

**DNA Specialist:** A forensic specialist who works with a CODIS Laboratory, who has authority to enter DNA profiles into CODIS. A DNA Specialist also has permissions to enter information related to DNA collections, profiling and CODIS upload into NamUs missing and unidentified person records.

**FDLE:** Florida Department of Law Enforcement.

**FOIA:** The Freedom of Information Act is a law that gives any person the right to request access to information from the federal government. It is often described as the law that keeps citizens “in the know” about their government.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**Forensic Odontology:** A branch of forensic medicine that deals with teeth and marks left by teeth (as in identifying criminal suspects, missing persons or the remains of a deceased person).

**Frankfort Horizontal Plane:** The Frankfort Horizontal plane is used in post mortem photography, as well as the photography of skulls used in facial reconstructions and composite sketches. The Frankfort Horizontal Plane minimizes distortion of the skull and facial features by ensuring that the face or skull is not pointing to the right, left, up or down. The Frankfort Horizontal Plane is represented in profile by a line between the lowest point on the margin of the orbit and the highest point on the margin of the auditory meatus.

**Full Edit:** Allows users to enter and edit all cases within the geographic area for which the user is activated.

**Full View:** Allows users to view both published and restricted cases within the geographic area for which the user is activated.

**Geographic Area:** the County of an individual state or territory, or combination of counties in which a user is activated for editing and enhanced viewing privileges within NamUs.

**HIPPA:** Health Insurance Portability and Accountability Act.

**IAFIS:** The Integrated Automatic Fingerprint Identification System (IAFIS) is a national fingerprint and criminal history system which provides automated fingerprint search capabilities, electronic image storage, and electronic exchange of fingerprints and responses.

**IDENT:** Automated Biometric Identification System – fingerprint database managed by US-VISIT.

**IN SITU:** Being in the original position; not having been moved or transferred to another location.

**Joint Automated Booking System (JABS):** The Joint Automated Booking System (JABS) is a computer system that helps federal law enforcement agencies book, identify, and quickly share information about persons in federal custody.

**Identity History Data:** Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual – considered part of Criminal Justice Information.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**Limited Edit:** Allows users to enter and edit cases on which they are associated as the case manager (CM) or Local Contact (LC).

**Law Enforcement Sensitive (LES):** Unclassified information of a sensitive and proprietary nature that if disclosed could cause harm by jeopardizing investigations, compromising operations, or causing harmful or life-threatening situations for law enforcement personnel, confidential informants, witnesses, or other members of the public.

**Limited View:** Allows users to view public information in all published cases within the NamUs database. Users with Limited Edit will not have access to view any fields or screens that are restricted from public view.

**Locus, Loci (p/):** A specific location (locus) or specific locations (loci) of a gene or DNA sequence on a chromosome.

**OCA:** OCA is an acronym used in NCIC which refers to the originating agency's case number.

**ORI:** An ORI is a nine-character identifier assigned by NCIC to an agency which has met the established criteria for ORI assignment. An ORI identifies an agency within the NCIC system and during NLETS transactions. An ORI identifies an agency by state and location within a state, and may indicate type of agency (sheriff's department, police department, court, district attorney, etc.). An agency may be assigned an ORI regardless of whether or not the agency has an NCIC terminal within their department.

**Medicolegal Death Investigator:** Someone responsible for conducting unnatural and unexplained death investigations such as homicides, suicides, unintentional injuries, drug-related deaths, and other deaths which are sudden or unexpected. A Medicolegal Death Investigator is usually associated with a medical examiner or coroner's office. He or she may be utilized for additional duties, such as odontology, anthropology, or other forensic analyses.

**Missing Child:** Any individual less than 18 years of age whose whereabouts are unknown to such individual's legal custodian (42 USCS § 5772; a missing person under the age of twenty-one may be considered a child under (42 USCS § 5779) requiring entry into NCIC.

**Missing Person:** A person 18 years or older whose disappearance is possibly not voluntary and whose whereabouts are unknown to criminal justice agencies, family members or NamUs staff.

# National Institute of Justice

## National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**Mitochondrial DNA:** Mitochondrial DNA is found in the cellular organelle called the mitochondria and is inherited only from the mother. Mitochondrial DNA is often referred to as “mito” and can be abbreviated as mtDNA.

**mtDNA:** See Mitochondrial DNA.

**NCIC (NIC):** The National Crime Information Center (NCIC) is the United States' central database for tracking crime-related information. Since 1967, the NCIC has been maintained by the Federal Bureau of Investigation's Criminal Justice Information Services Division, and is interlinked with similar systems that each state maintains. Data is received from federal law enforcement agencies, state and local law enforcement agencies, tribal law enforcement agencies, railroad police, and other agencies, such as state and federal motor vehicle registration and licensing authorities.

**NCMEC:** National Center for Missing & Exploited Children.

**Nuclear DNA:** Is found in the nucleus of the cell and is inherited from both the mother and father. Nuclear DNA profiles include STR (short tandem repeat) and Y-STR (Y-chromosome short tandem repeat) profiles.

**Odontologist:** A dentist specializing in the study of the structure, development, and abnormalities of the teeth.

**Pending Case:** Any case in the NamUs Missing Person or Unidentified Person database queues that is labeled as “New”, “Accepted”, “Incomplete” or “Pending ME/C Approval”. Pending cases are only visible to users with RSA or NamUs Staff access levels.

**Pending ME/C Approval:** An Unidentified Person (UP) is a case which meets all requirements for submission to a case manager or RSA, but has not been submitted to NamUs by the entering agency.

**Public User:** Any user not meeting the qualification of a U.S. Criminal Justice User. All users that are not public users are criminal justice users.

**Personally Identifiable Information (PII):** Information which can be used to distinguish or trace an individual's identity. PII includes – but is not limited to —name, social security number, biometric data, place of birth and other information which, alone or combined with other PII, can identify a specific individual.

**Published Cases:** Cases entered into NamUs, vetted by an RSA, and made viewable to the public.

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**Restricted Cases:** Cases that an entering or investigating agency wishes to be restricted from public view in NamUs due to LES/CJI.

**RFO:** Regional Forensic Odontologist employed by UNTHSC.

**RSA:** Regional System Administrator employed by UNTHSC or NCMEC.

**SME:** - A subject-matter expert (SME) is a person who is an expert in a particular area or topic.

**Suzanne's Law:** "Suzanne's Law" was passed as part of the PROTECT Act of 2003. Named after 19-year-old missing college student Suzanne Lyall, "Suzanne's Law" eliminates waiting periods before law enforcement can take a missing child report and investigate the disappearance of a missing child. The law also changed the definition of a child to anyone under the age of 21, and mandates the entry of all missing children under 21 into NCIC. NCMEC will accept cases of missing children aged 18 to 20 that are reported to them by a law enforcement agency, and refers to these cases as "5779 cases", which is in reference to 42 USC § 5779(c).

**STR:** Short Tandem Repeats (STRs) are short sequences of DNA that are repeated numerous times in a head-tail manner. Also see Nuclear DNA and Autosomal DNA.

**System:** Refers to connections, information repositories, equipment used to establish connections, applications and all interconnecting infrastructure required to use those applications related to NamUs.

**TXDPS:** Texas Department of Public Safety.

**Unidentified Human Remains:** The remains of a deceased human that cannot be identified as being associated with a previous living individual.

**Unpublished Cases:** Cases entered into NamUs, but not publicly viewable. All new cases entered into NamUs remain unpublished until they are vetted by the RSA and the RSA obtains permission to publish by the investigating agency.

**UNTCHI:** The University of North Texas Center for Human Identification (UNTCHI) is a national resource for the identification of missing and unidentified persons, combining the services of a forensic DNA laboratory, a forensic anthropology laboratory, and the Forensic Services Unit (FSU).

## National Institute of Justice

### National Missing and Unidentified Persons System (NamUs) Policy Manual - Version 1.0

**UNTHSC:** University of North Texas Health Science Center serves as home to several National Institutes of Health-funded research programs, as well as the NamUs and missing person DNA programs funded by the National Institute of Justice.

**Unverified Cases:** Cases entered into the NamUs Missing Person (MP) database which cannot be validated with criminal justice agencies as legitimate missing person cases.

**USCIS:** United States Citizenship and Immigration Services (USCIS) is a component of the United States Department of Homeland Security (DHS). It performs many administrative functions formerly carried out by the former United States Immigration and Naturalization Service (INS), which was part of the Department of Justice. USCIS is headed by a director who reports directly to the Deputy Secretary for Homeland Security.

**US-VISIT:** United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is a program of the Department of Homeland Security. US-VISIT provides biometric identification services to federal, state and local government agencies to help them accurately identify the people they encounter and determine whether those people pose a risk to the United States.

**ViCAP:** The Violent Criminal Apprehension Program, a program of the Federal Bureau of Investigation. It is designed to collect and analyze information about homicides, sexual assaults, missing persons, and other violent crimes involving unidentified human remains.