Privacy Impact Assessment
for the

National Child Victim Identification System (NCVIS)

August 21, 2009

Contact Point
Kumar Kibble
Acting Director, Office of Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The National Child Victim Identification System (NCVIS), owned by U.S. Immigration & Customs Enforcement (ICE), is an application that assists Federal, State, local, and international law enforcement agencies during investigations of child sexual exploitation crimes, specifically those involving images of child exploitation. NCVIS maintains a repository of electronic images of child exploitation submitted by law enforcement agencies. These images may capture the faces or other identifying features of the victims of these crimes and the violators. The primary purpose of NCVIS is to provide a means of connecting law enforcement personnel seeking to identify child victims in an image with law enforcement personnel who have already identified the victim in the image. A secondary purpose is to identify identical or substantially similar images to assist in identifying the child victims and to promote coordination among law enforcement agencies working on related investigations. ICE conducted this Privacy Impact Assessment because of the highly sensitive nature of the NCVIS images. Other than the images themselves, NCVIS does not maintain the identities of the child victims or violators.

Overview

Purpose and Use of NCVIS

ICE created NCVIS as a proactive investigative tool to assist Federal, state, local, and international law enforcement agencies during investigations of child sexual exploitation crimes, specifically those involving images and videos of child exploitation.[1] For purposes of NCVIS, images of child exploitation are defined using the statutory definition of "child pornography," which means any visual depiction, such as a photograph, film, video, or picture, of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.[2] (*See 18 U.S.C. 2256(8)(A)*).

Due to the exploitative nature of the crimes they depict, the digital images contained in NCVIS are highly sensitive and are maintained, used, and accessed for law enforcement purposes only. The primary purpose of NCVIS is to provide a means of connecting law enforcement personnel seeking to identify child victims in an image with law enforcement personnel who have already identified the victim in the image. The system aids the prosecution of these crimes by making it possible for law enforcement

[1] In addition to owning and operating NCVIS, ICE's Office of Investigations also conducts its own criminal investigations of child pornography. ICE may submit images from its investigations to NCVIS, through the National Center for Missing and Exploited Children described below.

[2] Although Federal criminal statutes use the term "child pornography," investigators use the term child exploitation in referring to these investigations and crimes. The term "pornography" connotes commercial or voluntary participation by the participants, as in adult pornography where the parties involved are willing participants and compensated in some manner. The children documented in child exploitation images are not participating of their own free will and are not compensated as an adult would be. The images are the documented evidence of a child being sexually exploited. Accordingly, throughout this document the term child exploitation will be used.

agencies to share information about related cases and determine the identity of child victims. NCVIS also assists law enforcement agencies in distinguishing between images of actual child exploitation and computer-generated/altered images. Establishing that an image of child exploitation contains an actual victim is important to preclude or answer a violator's claims at trial that the image was computer-generated or altered and does not depict crimes against an actual child. NCVIS is a cooperative effort among Federal, state, local, tribal and foreign law enforcement agencies, and the National Center for Missing & Exploitation Children. NCVIS is managed and administered by the ICE Office of Investigations (OI) Cyber Crimes Center.

NCVIS contains three primary types of information: digital images submitted by law enforcement investigators, unique image signatures generated by the system, and limited information related to the law enforcement investigation. As mentioned above, digital images fall into two categories – confirmed and unconfirmed – depending on whether the image is of an actual, known (i.e., confirmed) victim or an unknown (i.e., unconfirmed) victim. Unique image signatures are generated for each image in NCVIS using various tools and are used to identify images that may be a match. Finally, NCVIS maintains a limited amount of case-related information about the criminal investigation for which the image was submitted. The case information does not include identifying information about the victim or violator such as their names, but does include limited victim information such as age at the time of violation and date of birth, if known.

Through NCVIS, ICE provides a service to law enforcement agencies that have seized images of child exploitation but do not know the identity of the victim, or if the image is real or computer-generated. Agencies may submit these images, known as "unconfirmed images," to ICE's Cyber Crimes Center and request they be compared against the NCVIS repository of images where the victim has been identified, known as "confirmed images." If NCVIS identifies an exact or close match, ICE provides the agency with a report containing information about the matching confirmed image, including the contact agency for the law enforcement investigator. This service allows law enforcement agencies to identify related cases and share information that furthers the prosecution of these crimes.

Processing of Confirmed Images

Confirmed images are collected by Federal, state, local, and international law enforcement agents during child exploitation investigations and forwarded to the National Center for Missing and Exploited Children (NCMEC) where they are received by a Federal law enforcement agent from ICE, the FBI, the U.S. Postal Service, or the Department of Defense. NCMEC is a congressionally-mandated, non-profit organization that serves as the official national resource center and clearinghouse for missing and exploited children.[3] Under the supervision of Federal law enforcement agents, NCMEC personnel enter the unique signatures of identified images in the NCMEC Child Recognition & Identification System (CRIS) which performs a service that is similar to NCVIS. They also redact the explicit portions of the images prior to storing them in CRIS with the unique identifier. The Federal law enforcement partners working at NCMEC then transfer the confirmed images to the ICE Cyber Crimes Center for inclusion in

[3] Congress directed NCMEC to "operate a child victim identification program in order to assist the efforts of law enforcement agencies in identifying victims of child pornography and other sexual crimes." 42 U.S.C. § 5773.

NCVIS. The Cyber Crimes Center then provides the confirmed images and case information to Interpol to aid in the international enforcement activities against child exploitation crimes.

Processing of Unconfirmed Images

When the Cyber Crimes Center receives a request from a law enforcement agency to compare an unconfirmed image with the NCVIS repository of confirmed images, NCVIS generates and stores a matching report.[4] The report identifies an exact or closest matching image that meets a predetermined threshold and displays it side-by-side with the unconfirmed image for visual comparison. To ensure accuracy, the system-generated match is visually confirmed by an ICE agent before the Cyber Crimes Center sends the report to the requesting agency. The matching report also contains the contact information of the investigator who submitted the confirmed image, the file names associated with the images, and the series name (assigned per NCMEC series naming protocol, which does not include any information that would identify the victim or violator) associated with the images. The report is used to connect investigators seeking to identify a child victim in a specific image with investigators who have already identified the victim in another investigation.

NCVIS detects computer-generated or altered images via the matching described above. It does not analyze individual images to determine whether they have been altered – this capability is performed by other unrelated ICE tools, systems, and specialists.

The images in NCVIS are never shared with non-law enforcement entities. The only NCVIS data that is shared outside of the law enforcement community is statistical reporting data such as the number of confirmed and unconfirmed images that have been submitted. Due to the nature of the images in NCVIS, system access is limited to ICE Cyber Crimes Center personnel and ICE agents who investigate child exploitation crimes.

Typical Transaction

A typical transaction in NCVIS occurs when law enforcement personnel, such as a local police officer, submits a seized image of child exploitation to the Cyber Crimes Center to determine whether the image depicts a known victim. The Cyber Crimes Center uses NCVIS to produce a matching report, which includes the submitted image, the closest matching image in the repository, and the contact information for the law enforcement officer able to identify the child. The Cyber Crimes Center then sends that report to the submitting law enforcement officer for use in the investigation and to aid prosecution. The report is stored in NCVIS as a record of the request and match result.

[4] ICE usually receives requests of this type only after NCMEC has been unable to identify an exact match between an unconfirmed image and a confirmed image in CRIS. Because NCVIS has additional image matching capabilities, these requests are usually referred to ICE once NCMEC is unable to find a match.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The NCVIS repository maintains digital images (still images and still video frames) of child exploitation seized as evidence during official law enforcement investigations. This includes both confirmed and unconfirmed images, as described in the Overview. NCVIS also maintains official contact information for the law enforcement personnel that submitted the images to NCMEC and the Cyber Crimes Center. For purposes of NCVIS, images of child exploitation are defined using the statutory definition of "child pornography," which means any visual depiction, such as a photograph, film, video, or picture, of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.[5] *See* 18 U.S.C. § 2256(8)(A).

Some images in NCVIS do not, when assessed independently, meet the definition of child exploitation but are included because they are part of a sequential series of images that include images of child exploitation. Such images may be useful in the matching process and assist in identifying the victim or violator. For example, a series of images may start with the child victim fully clothed and progress to images of child exploitation as defined above. The determination whether an image or series constitutes child exploitation is made by the investigating law enforcement officer that submitted the image based on training and experience.

NCVIS generates and stores unique signatures of the images and still video frames in its repositories. These signatures serve as unique identifiers specific to each image or video frame. The system uses the signatures to analyze and compare images and to limit the need for system users to view the actual images and video.

NCVIS maintains a limited amount of case-related information about the criminal investigation for which the image was submitted, including the submitting agency's case number, the victim's date of birth (for confirmed images only), date of seizure, date and location of image (if known), violator's relationship to the victim, violator's means of accessing the Internet (including their screen name), the mechanism used to create the image (i.e., cell phone, digital camera), the name of the publication where it appeared, the URL where it was found, the email address of the individual who sent and/or received the image, NCMEC's case number, the series name (used by both perpetrators and law enforcement

[5] Although Federal criminal statutes use the term "child pornography," investigators use the term child exploitation. in referring to these investigations and crimes. The term "pornography" connotes commercial or voluntary participation by the participants, as in adult pornography where the parties involved are willing participants and compensated in some manner. The children documented in child exploitation images are not participating of their own free will and not being compensated as an adult would be. The images are the documented evidence of a child being sexually exploited. Accordingly, throughout this document the term child exploitation will be used.

worldwide to identify a particular series of images), and whether or not the images were distributed. NCVIS also stores the contact information for the law enforcement investigator who submitted the images. This contact information includes the investigator's name, agency, official phone and fax number, official email address, and official mailing address.

In response to requests from Federal, state, local, and international law enforcement personnel to assess whether an unconfirmed image matches any of the images in the NCVIS repository, the system generates matching reports that include the submitted unconfirmed image and the exact or closest matching confirmed image, the contact information for the investigator that submitted the confirmed image to NCVIS, the file name of the image, and the series name of the image. The reports do not contain any other information.

NCVIS stores the confirmed images, unconfirmed images submitted for matching, and the matching reports that are generated. Other than the images and the information described above, there is no other identifying information about the victim or violator stored in NCVIS.

1.2 What are the sources of the information in the system?

Federal, state, local, and international law enforcement personnel are the source of the images in NCVIS. They seize the images as evidence in the course of criminal investigations. Confirmed images are sent to NCMEC along with the case information described in Question 1.1 above. The ICE liaison agent at NCMEC delivers the confirmed images to the Cyber Crimes Center for inclusion in NCVIS. Law enforcement personnel send unconfirmed images directly to the Cyber Crimes Center for comparison against the NCVIS repository of confirmed images, primarily when NCMEC was unable to identify a match using their own matching system.

NCVIS is itself the source of information for the matching reports.

1.3 Why is the information being collected, used, disseminated, or maintained?

The primary purpose of NCVIS is to provide a means of connecting law enforcement personnel seeking to identify child victims in an image with law enforcement personnel who have already identified the victim in the image. The confirmed images are collected and maintained as a repository of identified victims to permit comparison to and matching with unconfirmed images. This system assists law enforcement investigators in determining if a child victim in their investigation has been identified, and to share case information with investigators in related cases. Records, information, or testimony from the law enforcement investigator that knows the identity of the victim may be provided and used in the investigation and prosecution of a criminal case. For example, the investigating officer in the original case may testify in subsequent cases about the images and the victim being a real child, not a computer-generated image. NCVIS also assists law enforcement agencies in distinguishing between images of actual child exploitation and computer-generated/altered images.

Law enforcement contact information and case-related information is maintained in NCVIS to allow the submitters of unconfirmed images to contact the submitters of confirmed images to aid in investigation and prosecution.

The NCVIS matching reports are created and maintained to provide an official record of the results of an exact or close match of an unconfirmed image to the NCVIS repository. The report is used by the submitting law enforcement investigator in the course of the investigation, and by the prosecutor as evidence in any criminal action against the alleged violator.

1.4 How is the information collected?

For confirmed images, law enforcement personnel first submit copies of the seized images, case-related information, and their official contact information to NCMEC. Law enforcement personnel typically send images to NCMEC in a digital format via procedures set forth by NCMEC. NCMEC provides specific submission instructions as well as a suggested template form to be used when submitting images. The ICE liaison agent assigned to NCMEC then delivers the confirmed images to the ICE Cyber Crimes Center for inclusion in NCVIS.

For unconfirmed images, law enforcement personnel send digital copies of the seized images, contact information, and related case information to the Cyber Crimes Center requesting a match against the confirmed images stored in NCVIS. There is no standard form used by all law enforcement agencies for submitting matching requests to NCVIS.

NCVIS itself generates and stores the unique signatures and the matching reports for the images.

1.5 How will the information be checked for accuracy?

The confirmed images contained in NCVIS are submitted by law enforcement personnel that have first hand accountings of the victim. The Cyber Crimes Center relies on these law enforcement agencies to provide only the appropriate images and accurate case information to NCMEC which provides them, in turn, to the Cyber Crimes Center. To prevent the unnecessary collection of information in the system, the NCVIS input fields are standardized.

If an authorized NCVIS user or authorized recipient of an NCVIS report discovers an image in the NCVIS repository that does not depict an actual victim, or if they discover inaccurate law enforcement personnel contact information in the NCVIS repository or an NCVIS report, correction requests can be submitted to NCMEC which will update their database with the corrected information. NCMEC will then notify the Cyber Crimes Center, which will make corrections to NCVIS.

The reports generated by NCVIS may be used as evidence in court to demonstrate to the jury how the victim depicted in a particular image of exploitation was identified as a real child. The jury has the opportunity to review the report and determine whether they believe the confirmed and unconfirmed images actually “match.” They also have the opportunity to hear and assess the testimony of the law enforcement investigator who is testifying about the victim depicted in the images of child exploitation. This process helps to ensure that incorrect information is unlikely to propagate, persist, or result in an inappropriate adverse action against an individual.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Crimes involving exploitation of children often involve international distribution; as a result investigations of these crimes are part of ICE's enforcement mission. *See* 6 U.S.C. § 203; 19 U.S.C. §§ 482, 1305, 1461, 1467, 1469, 1499, 1509, 1583, and 1589a; DHS Delegation No. 7030.2, "Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement" (Nov. 13, 2004). These images are collected as part of ICE's role in assisting in Federal, state, local, and international detection and prosecution of crimes falling under 18 U.S.C. § 2251 et seq. Additionally ICE formalized its arrangement with NCMEC in a Memorandum of Understanding (MOU) on June 22, 2004 to aid in the collection of child exploitation images for law enforcement purposes.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: The images stored in NCVIS are extremely sensitive due to their explicit nature, the fact that the victims are minors, and the fact that these images are evidence of criminal activity. This privacy risk associated with maintaining these images are that the individuals in the images would be able to be identified if NCVIS were compromised or access by an unauthorized person or for unauthorized purposes.

Mitigation: NCVIS does not collect or maintain any identifying information about the individuals involved in these crimes beyond the images themselves, except for the victim date of birth and age at the time of violation if known, the violator's screen name and email address, and the relationship between the violator and the victim. Additionally, NCVIS uses technology that substantially reduces the instances in which images of child sexual exploitation are viewed for law enforcement purposes. These limitations reduce the risk to the privacy of the individuals depicted in these images.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

ICE and other law enforcement agencies use NCVIS as a repository of images and video stills of child sexual exploitation to assist in the prosecution of these crimes. The system matches unconfirmed images of unidentified victims to confirmed images of identified victims, and the reports produced provide a means of connecting law enforcement personnel seeking to verify that a child is real with law enforcement personnel who have already identified the victim in the image. Unique signatures of the images are used for purposes of image analysis and comparison.

Law enforcement contact information is used to identify the officer able to verify that the imaged child is real, and to facilitate contact among law enforcement agencies about the distribution of known images in other investigations. Case-related information is used to prepare the case for criminal prosecution.

NCVIS-generated matching reports are used by investigators and prosecutors in the investigation and prosecution of these crimes. The reports may be entered into evidence during criminal trials to demonstrate how the law enforcement authority identified a victim depicted in a particular image is a real child.

2.2 What types of tools are used to analyze data and what type of data may be produced?

NVCIS contains several tools to aid law enforcement agents in identifying and cataloging images of child sexual exploitation. It creates a unique signature for each image and video still to easily identify matches. The NCVIS repository stores the digital image and video stills along with their system-generated unique signatures.

After NCVIS compares the images using the unique signatures, the system generates a matching report that includes the images side-by-side. The ICE agent running the report visually compares the images to ensure they are the same, thereby eliminating the chance that any false positive matches will be released. Law enforcement officers, prosecutors, and juries may also compare and verify that images are the same.

The NCVIS image matching program can be used in single image or batch image requests. When a request comes in to match multiple images, the system processes the images and generates a separate matching report for each request. This utility saves time by performing batch image matching requests with report generation.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

NCVIS access is limited to ICE agents who use it while conducting official criminal child exploitation investigative activities. As described in Section 8 of this PIA, security and access controls are in place to mitigate the risk of unauthorized individuals gaining access to information in the system. Users take mandatory annual privacy and security training, which stresses the importance of authorized use of personal data in government systems. Individuals who are found to access or use NCVIS data in an unauthorized manner will be disciplined in accordance with ICE policy, and may be subject to criminal

sanctions for misuse of Federal information systems. These and other controls described in this PIA ensure the system is used only by authorized users for the intended purpose.

In addition to the standard security controls associated with highly sensitive data, NCVIS uses automated image matching software. This greatly reduces the need for law enforcement officers to view the images. Once close or exact matches are identified, the law enforcement officer can inspect the images manually to ensure that NCVIS has not produced a false positive. The report generated by NCVIS includes a side-by-side display of both the submitted image and the closest match thereby further preventing erroneous matches from being used as evidence.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

NCVIS retains all images of child sexual exploitation (both confirmed and unconfirmed images), unique signatures, case-related information, and law enforcement officer contact information. NCVIS also retains the matching reports.

3.2 How long is information retained?

In accordance with the approved records schedule, hard copies of images and associated data are destroyed after the information has been converted to an electronic medium and verified, when no longer needed for legal or audit purposes or to support the reconstruction of, or serve as a backup to, the electronic records. Electronic copies of the images and associated data are deleted 99 years after entry into system, and only after verification that it is not part of any legal hold, and no longer needed for business purposes.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Retaining NCVIS data longer than necessary would violate the Fair Information Principle of minimization which requires systems and programs to retain only the information necessary and relevant to complete the task associated with its initial collection.

Mitigation: The retention period is necessary to support the law enforcement and evidentiary purposes for which the system exists. The distribution and viewing of this material is a crime regardless of how old the image itself is. Given the ease with which criminals can replicate, distribute and otherwise perpetuate these electronic images, it is reasonable to expect that law enforcement will have a continuing need to use NCVIS to identify these images in support of law enforcement investigations and prosecutions for many years after the image was created.

Privacy Risk: The long retention period of NCVIS records increases the risk that they will be misused or disclosed.

Mitigation: NCVIS is only accessible to Cyber Crimes Center personnel. Further, a variety of technical and administrative controls (described throughout this PIA) reduce the risk that NCVIS will be misused or that NCVIS data will be shared inappropriately.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

ICE may share NCVIS data on an ad hoc basis with other DHS law enforcement agencies when those agencies submit an unconfirmed image to the Cyber Crimes Center requesting a match. This only occurs in the context of law enforcement investigations of child exploitation violations by official DHS law enforcement personnel. The Cyber Crimes Center will share the NCVIS matching report documenting any match between the submitted unconfirmed image and the matching confirmed image in the NCVIS repository.

4.2 How is the information transmitted or disclosed?

NCVIS matching reports are sent to DHS law enforcement officers in an encrypted password-protected Portable Document Format (PDF) file. Normally the encrypted file is burned to a CD-ROM, double enveloped and sent by a traceable courier to the law enforcement personnel handling the case. The password is sent under separate cover to the case agent.

Once the DHS law enforcement officer receives the NCVIS report, they handle the information according to their internal agency policy. This usually includes establishing and keeping a secure chain of custody record, and marking the material as evidence that may be used in a trial.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: There is a risk that the information may be used by recipients for purposes other than those for which the information is shared.

Mitigation: ICE only shares information from NCVIS in the context of investigations of child exploitation with other law enforcement agencies. Recipients of this information are trained law enforcement personnel who handle it pursuant to strict evidentiary standards.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ICE may share NCVIS data outside of DHS on an ad hoc basis with other Federal, state, local or international law enforcement agencies when those agencies submit an unconfirmed image to the Cyber Crimes Center requesting a match. This only occurs in the context of a law enforcement investigation of child sexual exploitation by the submitted agency. The Cyber Crimes Center will share the NCVIS matching report documenting any match between the submitted unconfirmed image and the matching confirmed image in the NCVIS repository. The Cyber Crimes Center also routinely provides confirmed images and case information to Interpol to aid in international enforcement activities against child exploitation crimes.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. The sharing of matching reports with law enforcement officers in support of child sexual exploitation investigations is the intended use of the system. The matching reports provide a means of connecting law enforcement personnel seeking to verify images of child victims with law enforcement personnel who have already identified the victim in the image. The report is used to further the investigation, and used as evidence in any criminal case that is brought to trial.

The information in NCVIS is retrieved by matching image files, unique file signatures, or other image characteristics. Information is not retrieved by any unique personal identifier. NCVIS is therefore not a system of records under the Privacy Act and does not require the publication of a system of records notice.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

NCVIS matching reports are sent to law enforcement officers in an encrypted password-protected Portable Document Format (PDF) file. Normally the encrypted file is burned to a CD-ROM, double enveloped and sent by a trackable courier to the law enforcement personnel handling the case. The password is sent under separate cover to the case agent.

Once the law enforcement officer receives the NCVIS report, the information is handled according to their internal agency policy. This usually includes establishing and keeping a secure chain of custody record, and marking the material as evidence that may be used in a court case.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: There is a risk that the information may be used by recipients for purposes other than those for which the information is shared.

Mitigation: ICE only shares information from NCVIS in the context of investigations of child exploitation with other law enforcement agencies. Recipients of this information are trained law enforcement personnel who handle it pursuant to strict evidentiary standards.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

This PIA serves as notice to the public of the existence of NCVIS system. Typically, victims and violators do not receive notice prior to the seizure of the contraband images and video, and their inclusion in NCVIS. In some circumstances, actual notice prior to seizure of the image may be provided to the violator by service of a search warrant, for example.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Given the law enforcement context in which this information is collected, there is no opportunity and/or right to decline to provide the images and video. These materials are potential evidence of criminal activity and are seized and used in accordance with the requirements of criminal law and procedures.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Given the law enforcement context in which this information is collected, there is no right to consent to particular uses of the information.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: A risk exists that the public is unaware of the existence of NCVIS or that victims may be unaware that these images are contained in NCVIS.

Mitigation: Notice is provided by the publication of this PIA, which provides a detailed description of the information contained in the system, its uses, and the safeguards in place to protect the information from improper use or disclosure. As previously noted, due to the law enforcement nature of these collections individuals are not provided with advance notice of the collection. However the safeguards described in this PIA pertaining to the collection, sharing and access to this material mitigate these risks.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

NCVIS does not contain information that identifies the victims or violators in the images it maintains. As such, it is not possible to retrieve from NCVIS a particular record based on the identity of the individual depicted. Further, the images contained in NCVIS are contraband and evidence and it is unlawful for anyone except law enforcement officers acting in their official capacities to view or possess the images. Accordingly, there are no procedures available for victims or violators to view or obtain copies of their own images in NCVIS.

7.2 What are the procedures for correcting inaccurate or erroneous information?

NCVIS does not contain information that identifies the victims or violators. Accordingly, there is no need for procedures to allow victims and violators to correct information in NCVIS.

Law enforcement investigators can submit corrections to their contact information or other case related information by communicating the change to NCMEC, which in turn notifies the NCVIS administrator. The administrator will update NCVIS to reflect the change.

7.3 How are individuals notified of the procedures for correcting their information?

The procedures for law enforcement officers to correcting their contact information are outlined in this PIA.

7.4 If no formal redress is provided, what alternatives are available to the individual?

No alternatives are available.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: No redress is available to individuals, including victims and violators, who are captured in images of child exploitation maintained in NCVIS.

Mitigation: Federal law prohibits the viewing or possession of these images by anyone other than law enforcement officers in the official conduct of their duties. NCVIS purposefully does not maintain victim or perpetrator identity information outside of the images themselves to eliminate the risk that their identities may be unnecessarily shared or compromised. As such, NCVIS contains no personally identifiable information about victims or violators for which correction could be sought.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Direct access to NCVIS is strictly controlled by the NCVIS program manager in cooperation with the system administrator. ICE law enforcement personnel requesting access to NCVIS must articulate their need for access in the performance of their official duties. This only occurs when an ICE agent is

involved in an investigation involving images of child exploitation or when ICE Cyber Crimes Center personnel are assigned to support NCVIS. Access to NCVIS is only granted upon review by the NCVIS program manager and system administrator. Any ICE personnel that requests access must have a superior submit a formal request to the NCVIS program manager for approval.

User access is controlled by the NCVIS administrators. The system restricts a user's data access rights depending on the level of permissions granted in accordance with the user's system profile (e.g. system administrator, content experts, search experts) according to the following table:

Table 1. System Roles

Role	Level of Access
System Administrator	Possesses read/write access to all data
Content Experts	Possesses specific read/write privileges granted by the system administrator. This role is usually delegated the Cyber Crimes Center personnel responsible for entering new confirmed images into the NCVIS repository that are received from NCMEC.
Search Experts	Possesses read-only ability of all content with no write access permissions. This role is usually delegated to the Cyber Crimes Center personnel responsible for using NCVIS to analyze an unconfirmed image and produce a matching report.

8.2 Will Department contractors have access to the system?

Yes. ICE NCVIS contractors have access to the system for the purpose of supporting image analysis as well as providing information technology services related to system development, maintenance, and operations. All contractors have appropriate security and suitability clearances prior to being granted system access.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All ICE personnel and contractors complete annual mandatory privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. Also all ICE agents are provided with general training on the sensitivity and appropriate use (e.g. victim identification, geographical background comparison/location identification, verification of identified child victim, evidence in court proceedings) of NCVIS when they join the agency. When the ICE personnel are given direct access to NCVIS, they also receive training on accessing the system and performing digital image analysis.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

NCVIS has a current Certification and Accreditation issued on September 26, 2006, and in effect for three years.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

DHS ICE law enforcement personnel access NCVIS. The NCVIS server is located on a secure, stand-alone network that exists at the ICE Cyber Crimes Center. This network is not connected to the DHS network. Users access NCVIS using two-factor authentication in the form of a VPN token that is only used to access the NCVIS network. VPN access requires a user account on the server, the VPN pass code, a valid user ID on the NCVIS network, and the password for the submitting user ID. VPN access is conducted through a firewall that enables encryption into the network, along with user authentication, permission monitoring, and user auditing.

NCVIS utilizes enclosed data communication lines and Storage Area Networks (SANs) located at the Cyber Crimes Center and at a back-up location. The data is stored and contained within their dedicated SANs and does not connect to the ICE enterprise network system. The NCVIS server is located in a keypad-isolated room that can only be accessed by system administrators, program managers and IT officers. Access to the door is restricted by proximity card. Server access requires an NCVIS account that is managed by the system administrator and NCVIS program manager.

User passwords are required for access to the NCVIS application. The user profiles defined in Section 8.1 limit user access to the data. All actions conducted on the system are logged and auditable. The system logs User ID, login time, login attempts, logoff time, failed login attempts, data records accessed, changed, and deleted. Periodic audits on system usage are conducted by the system administrator in coordination with the NCVIS program manager.

Images stored in NCVIS are encrypted using Triple DES, which provides additional protection to the data and prevents system administrators from viewing the data while managing the system.

In addition, NCVIS was specifically designed to reduce the need for users to be exposed to the images in NCVIS. Additionally, the system's image matching capabilities also automate a significant amount of the image matching work and, thereby, reduce the exposure of ICE agents to the contraband images and reduce the likelihood of misuse.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: The images stored in the database are highly sensitive. Misuse and/or inappropriate disclosure represent a significant privacy risk to the individuals depicted in the images.

Mitigation: Appropriate security measures including limited, role-based access, two-factor authentication, and use of a stand-alone system not connected to other networks provide robust security for the sensitive data in the system. Also, users are required to have additional background checks performed prior to being granted system access. Images stored in NCVIS are encrypted using Triple DES, which provides additional protection to the data and prevents system administrators from viewing the data while managing the system. Finally, no identifying information is stored in the system, which greatly reduces the risk of embarrassment or other harm to any victim whose images are stored in the system.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

NCVIS is a system with data analysis tools supporting the identification of victims of child exploitation to facilitate the prosecution of crimes involving child exploitation.

9.2 What stage of development is the system in and what project development lifecycle was used?

NCVIS is currently in the Operations and Maintenance phase. The system was developed under the general guidance of ICE's Software Lifecycle Management Handbook.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The system automates image matching using image analysis software. The software will identify the closest match to any submitted image. It is possible that the closest match reported by NCVIS does not represent the same image. This risk is mitigated by the fact that all NCVIS results are reviewed by authorized Cyber Crimes Center personnel to ensure that a match is a true match. Even if a "false-positive" is not detected by Cyber Crimes Center personnel, the law enforcement personnel who receive the report will review it to ensure that it documents a true match. After that, the relevant attorneys for the law enforcement agency prosecuting the case will review the evidence to ensure it documents a true match. Finally, the jury or judge at trial will review the evidence to ensure that it documents a true match.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security