Drug Enforcement Administration

Privacy Impact Assessment
for
Case Cracker Interview Room Video

Issued by:
James Robert Bryden
DEA Senior Component Official For Privacy

Approved by: Michelle Ramsden
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 23, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The DEA installed the Cardinal Peak Case Cracker Interview Room Recording System (Case Cracker) to assist users in conducting live, consensual interviews between DEA investigators and potential targets or other individuals interviewed on the premises of DEA locations in designated interview rooms. Upon activation, the system has the option to record or "live monitor" without recording.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The Case Cracker interview room system records live, consensual interviews between DEA investigators, DEA task force officers, and potential targets or other individuals interviewed on the premises of DEA locations in designated interview rooms. Each interview room equipped with the system will have two cameras and two microphones which carry recorded data back to a standalone server at present. In the future, it is possible that the information will be uploaded to the Firebird network[1]. The session is started by pressing a button outside the room to begin the interview and subsequently pressing the button to end the session when the interview is complete. Upon activation, the system has the option to record or "live monitor" without recording. The system does not create any metadata. However, the interviewing agent can subsequently input whatever metadata is deemed important—the file may then be searched by any entered metadata.

Each DEA location equipped with Case Cracker will have the system running on a centralized local server capable of housing data for up to three interview rooms. Case Cracker does have network capability but, DEA has not employed the network option at this time (in the future it is possible that the Firebird Network will be used). Additionally, Case Cracker has no connection to the internet. After activating Case Cracker to record interviews, Special Agents are granted permission to download an official copy of the interview by the designated on-site System Administrator to permissible removable media (DVD, thumb drive, external hard disk, etc.) Once labeled, a copy is stored in the relevant evidence storage area. As DEA moves into deploying the network capabilities of Case Cracker, this paragraph will be updated to reflect any new architecture.

Case Cracker is used for collecting, maintaining, using, and distributing video and audio recordings pertaining to consensual custodial face-to-face interviews conducted for investigative purposes in DEA interview rooms. The types of information that are collected, maintained, used, and

[1] The DEA Firebird network is covered by separate compliance documentation.

disseminated by Case Cracker is dependent upon the questions asked or information disclosed by the interviewee during the actual interviews. However, basic background information of the interviewee (e.g., names, aliases, addresses, etc.) would generally be recorded as would statements or recollections, if any, regarding events of interest obtained for investigative purposes. DEA also may collect information pertaining to United States (U.S.) citizens, lawfully admitted permanent resident aliens, and non-U.S. citizens.***2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)***

Authority	Citation/Reference
Statute	The Comprehensive Drug Abuse Prevention and Control Act of 1970 (Controlled Substances Act), 21 U.S.C. § 801 et. seq.; See also, 44 U.S.C. § 3502 and 40 U.S.C. § 11101
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	May 12, 2014, Deputy Attorney General Memorandum, *Policy Regarding Electronic Recording of Statements; JM 9-13.001*

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Name	X	A, B, C, & D	Names of members of the public (USPERs and non-USPERs) are likely to be collected specific to an investigation; names also could be incidentally collected of employees, contractors, and other federal government personnel.
Date of birth or age	X	A, B, C, & D	* Note: Hereinafter asterisks indicate that collected information (US or non-USPERs) could incidentally include any type of content. Not all of these types of information are routinely contained in data collected. Such information of employees, contractors, and other federal government personnel also could be collected incidentally in some instances.
Place of birth	X	A, B, C, & D	*
Gender	X	A, B, C, & D	Genders of members of the public (USPERs and non-USPERs) is likely to be collected specific to of an investigation; the genders of employees, contractors, and other federal government personnel also could be collected incidentally.
Race, ethnicity, or citizenship	X	A, B, C, & D	*
Religion	X	A, B, C, & D	*
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, & D	*
Tax Identification Number (TIN)	X	A, B, C, & D	*
Driver's license	X	A, B, C, & D	*
Alien registration number	X	A, B, C, & D	*
Passport number	X	A, B, C, & D	*
Mother's maiden name	X	A, B, C, & D	*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Vehicle identifiers	X	A, B, C, & D	Vehicle identifiers of members of the public (USPERs and non-USPERs) may be collected specific to an investigation; Such information of employees, contractors, and other federal government personnel also could be collected incidentally.
Personal mailing address	X	A, B, C, & D	*
Personal e-mail address	X	A, B, C, & D	*
Personal phone number	X	A, B, C, & D	Phone numbers of members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
Medical records number	X	A, B, C, & D	*
Medical notes or other medical or health information			
Financial account information	X	A, B, C, & D	Financial account information of members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
Applicant information			
Education records			
Military status or other information	X	A, B, C, & D	*
Employment status, history, or similar information	X	C & D	Employment status, history or similar information of members of the public (USPERs and non-USPERs) may be collected specific to an investigation.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A, B, C, & D	Electronic device identifiers of members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
Web uniform resource locator(s)	X	A, B, C, & D	Information related to web uniform locator (s) information by members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information relative to employees, contractors, and other federal government personnel would be collected incidentally.
Foreign activities	X	C & D	Information related to foreign activities by members of the public (USPERs and non-USPERs) may be collected specific to an investigation.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Criminal history information of members of the public (USPERs and non-USPERs) may be collected incidentally.
Juvenile criminal records information	X	C & D	Juvenile criminal history information of members of the public (USPERs and non-USPERs) may be collected incidentally.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, & D	*
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, & D	Information related to witnessing criminal matters by members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information relative to employees, contractors, and other federal government personnel would be collected incidentally.
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, & D	Photographs and photographic identifier of members of the public (USPERs and non-USPERs) may be collected as elements of a video specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
- **Video containing biometric data**	X	A, B, C, & D	Videos, voice recordings and any biometrics-related information inherent in such video of members of the public (USPERs and non-USPERs) may be collected specific to an investigation, however no videos are intentionally obtained for biometric identification; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
- **Fingerprints**			
- **Palm prints**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Iris image**	X	A, B, C, & D	Video images of the irises of members of the public (USPERs and non-USPERs) may be collected specific to an investigation, however no iris images are intentionally obtained for biometric identification; such iris information of employees, contractors, and other federal government personnel also could be collected incidentally.
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, & D	Voice recordings and voice signatures. of members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
- **Scars, marks, tattoos**	X	A, B, C, & D	Identifiable scars mark and tattoos of members of the public (USPERs and non-USPERs) may be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A & B	PII of Employees/contractors.
- **User passwords/codes**			
- **IP address**	X	A & B	PII of Employees/contractors.
- **Date/time of access**	X	A & B	PII of Employees/contractors.
- **Queries run**	X	A & B	PII of Employees/contractors.
- **Contents of files**	X	A & B	PII of Employees/contractors.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, & D	Possible instances of as yet unknown PII related information may be incidentally collected of members of the public (US or non-USPERs), or of employees, contractors, other federal and government personnel.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure

electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			Via removable media or electronic transmission for the purpose of litigation.
DOJ Components	X			Via removable media or electronic transmission for the purpose of litigation.
Federal entities	X			Via removable media or electronic transmission for the purpose of litigation.
State, local, tribal gov't entities	X			Via removable media or electronic transmission for the purpose of litigation.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Via removable media or electronic transmission for the purpose of litigation.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

General notice of the existence and uses of Case Cracker is provided by the publication of this PIA and the applicable System of Record Notice (SORN). When law enforcement agents and officers interact with individuals in connection with an investigation, the subjects are generally aware that their information will be recorded and stored. The interviewee is informed that the interview is recorded.

Case Cracker operates as a supplement to the general case file system of DEA covered by SORN DOJ/DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012). That system of records contains law enforcement intelligence and investigative information in paper and/or electronic form, including information compiled for the purpose of identifying criminal, civil, and regulatory offenders; reports of investigations; identifying data and notations of arrest, the nature and disposition of allegations and charges, sentencing, confinement, release, and parole and probation status; intelligence information on individuals suspected to be violating laws and regulations; fingerprints and palmprints; laboratory reports of evidence analysis; photographs; records of electronic surveillance; seized property reports; and polygraph examinations.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

All interviews are consensual, so every interview presents the opportunity for individuals to participate in the collection of the information. The Case Cracker is a system accessed exclusively by Law Enforcement (LE) or other associated individuals in direct support of LE operations. Individuals subject to being interviewed will not have access, unless required for discovery pursuant to a civil litigation or criminal prosecution. At this time, Case Cracker is only used for custodial interviews. Since, under the 5th Amendment to the Constitution, no person is required to speak when interviewed and therefore, the subject does participate in whether any substantive collection of information occurs or not with Case Cracker.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

An individual may gain access to his or her information via an appropriately filed Freedom of Information Act (FOIA) request. DEA's public facing website contains a FOIA/PA webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. However, much of the information within DEA's Investigative Reporting and Filing System, covered by SORN DOJ/DEA-008, was made exempt by the Attorney General at 28 C.F.R. §16.98 from the Privacy Act disclosure, amendment, and correction provisions, pursuant to operation of 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Further, records compiled for law enforcement purposes are also excluded from production under the Freedom of Information Act (FOIA) 5 U.S.C. §552(b)(7). In evert of an

administrative, civil of criminal action against an interviewee, the individual may request a copy of the interview to be provided through the discovery process.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** Currently we are working on control assessment of this system to obtain an ATO. Anticipating ATP submission: 10/19/2023 Expected ATO completion date: 04/30/2026. **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No privacy related POA&Ms currently.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Case Cracker is assigned the security category of Moderate as defined in FIPS 199 based on the information type: Criminal Investigation and Surveillance.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle.

	DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the CPCLO, or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The Case Cracker system creates audit logs for all access to each account and all video viewing within that account. These auditing trails can be reviewed at any time by authorized DEA supervisors with the necessary permissions.
	Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:

6.2 ***Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?***

Physical Security Controls:

The Case Cracker storage server is housed in a secure location in an IDF/server room which cannot be accessed without a PIV card and access code. Only authorized personnel are given access to the IDF/server room. Authorized users are ones who have requested and been granted access to IDF/Server room.

Technical System Protections:

On-site technical personnel are designated as System Administrators. Only Administrators can make changes to the system, such as moving or deleting files.

Administrative Access Controls:

The types of users with access to information within the system are internal DOJ employees, contractors, and deputized Task Force Officers or other approved Federal Government

employees working with DEA on investigations. Only authorized users have access to this data/system using their userID/password. Authorized users are ones who have requested and been granted access to the system and been issued a logon and password.

The on-site System Administrators will give a type of limited system access to agents/officers only for making copies and downloading copies to encrypted removable media. It is also the Administrators' responsibility to construct a mandatory back-up system (such as a connected back-up server, or external hard drives, etc.) as well as to maintain regular monitoring of Case Cracker to ensure all of the important system and software updates are managed and received for continued functionality.

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

The Case Cracker system itself does not function as a repository for videos recorded. All files of videos on the system are purged after 60 days and the default rubric for identifying video session files added to servers within the last 60 days is the time/date at each location. Unless and until an interviewing Special Agent inputs what metadata he or she believes to be relevant, there is no capacity to recall files other than time/date. While any metadata entered can be used to locate these temporary video files, the standard operating procedure is for case agents to promptly (within 60 days) download the video from the Case Cracker server onto removable media (which will include a version of the propriety Case Cracker video-player and the session's video data). This will become the official record of the interview.

Once video is exported onto removable media it is placed into non-drug evidence and the removable media is then maintained in a system of records because it becomes associated with a case file, which the non-drug evidence custodian will use to retrieve the media. These media files are covered by SORN DEA-008, "Investigative Reporting and Filing System."

DFN 601-38a2 - https://intranet13.shpt.sbu.dea.doj.gov/sites/sa/sarr/dearis/Pages/App600.aspx

Nondrug Property

These files consist of various DEA forms (DEA-7a, DEA-7b, DEA-12, DEA-48a), ENEDS/CERTS printouts, abandonment correspondence(s), inventory records and other relevant information for tracking seized or abandoned nondrug property. Also included in these records are the court orders and other correspondence(s) related to Title III material. Disposition: Temporary. Cutoff at the close of the file annually. Destroy 2 years after close of file.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether

information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 ***Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012) (full text); 82 Fed. Reg. 24151, 156 (May 25, 2017) (amendment).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

a. Potential Threats Related to Collection of the Information

Risk: Agents may not define the parameters for interview topics and potential uses of the collected information in potential prosecution which could impair an individual's ability to fully consent to the information collection.

Mitigation: This risk is mitigated. Agents clearly define the parameters for each interview and subjects agree to such interview. Agents are provided training for conducting interviews as per DEA/DOJ policies and procedures.

Privacy Risk: PII may be inadvertently collected for investigations or activities beyond the scope of DEA's Title 21 authority.

Mitigation: This risk is mitigated. An agent's use of Case Cracker must be approved by appropriate supervisory personnel as part of investigatory activities that would also have been authorized by supervisors wherein any Title 21 authority issues would be addressed. In the unlikely event, information was collected that clearly beyond DEA's Title 21 authority, DEA would redact such information.

Privacy Risk: There is a possibility that the PII of an unrelated individual (who is not under suspicion or the subject of investigation) is collected as part of an incident or investigation about someone else.

Mitigation: This risk is mostly mitigated. In the unlikely event that the PII information for an unrelated individual were collected, then that information would be redacted in accordance with DEA's Title 21 authority. If information is incidentally obtained about others not involved in an incident or investigation, every effort will be made to redact such information. DEA will only retain third party information that is associated with those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or for identifying individuals or entities of concern.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: There is a risk of technological breach or unauthorized access to the recordings during transfer to storage and while in storage.

Mitigation: This risk is mitigated. Administrative access controls exist for Case Cracker limiting who can use the system. The types of users with access to information within the system are Federal Government employees, detailees and contractors. On-site technical personnel will be the designated System Administrators. Only Administrators can make changes to the system, such as moving or deleting files. The Administrators will give limited system access to agents/officers for viewing, making copies and downloading copies to encrypted removable media. It is also the Administrators' responsibility to construct a mandatory back-up system (such as a connected back-up server, or external hard drives, etc.) as well as to maintain regular contact with Case Cracker to ensure all of the important system and software updates are managed and for functionality.

Privacy Risk: Authorized DEA personnel may mishandle or fail to safeguard PII without adequate training.

Mitigation: This risk is mitigated. DEA reiterates the importance of safeguarding PII, during each Case Cracker training session. In addition, each user annually is required to review and acknowledge the DOJ and DEA IT Rules of Behavior as part of the mandated online IT Security Training. These individuals confirm they have read and accepted the IT Rules of Behavior regarding the proper handling of all DEA documents and data.

Privacy Risk: DEA's monitoring, testing and evaluation of privacy and security controls may be insufficient to protect the PII contained within Case Cracker.

Mitigation: This risk is mitigated. For the Case Cracker system, the monitoring, testing, and evaluation functions are conducted as required by NIST SP 800-53 Rev 5 and laid out in the System Security and Privacy Plan. Further the physical, technical and administrative controls referenced in Section 6.2 are subject to independent assessment of implementation as part of the Authorization to Operate process.

c. Potential Threats Related to Dissemination

Privacy Risk: There is a potential risk to privacy that could result from the potential unauthorized disclosure of the information within or from the Case Cracker program.

Mitigation: This risk is mitigated. . Case Cracker does not connect with other systems and any dissemination of information must be accomplished manually by downloading files from the system into removable media devices. The information collected by the program may be shared within DEA, the Department, Federal, state, local, tribal, and territorial agencies, as well as opposing counsel for purposes of criminal prosecutions. The types of users with access to information within the system is the Federal Government and the Local Police Department. On-site tech personnel will be the designated System Administrators. Only Administrators can make changes to the system, such as moving or deleting files. The Administrators will give limited system access to agents/officers for making copies and downloading copies to encrypted removable media. Agents and officers are trained to ensure disseminations are shared only with those authorized to receive them for legal and authorized purposes.