Drug Enforcement Administration

Privacy Impact Assessment
for the
Callyo Communications Application Suite

Issued by:
Robert McGovern
DEA Senior Component Official for Privacy (Acting)

Approved by: Kemeron Cox
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: November 16, 2026

(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 Callyo communications application suite (Callyo) assists users in conducting consensually recorded phone or video calls and face-to-face conversations with investigative targets. Callyo provides audio and video capabilities both covertly or overtly from any iPhone, Android phone, or laptop computer. Callyo's capabilities permit the documenting of special operations, field interviews, knock and talk investigations,[1] as well as in custody field interviews.

The data generated from the live stream can be viewed by agents in the field via a cellular smart phone device, laptop, or tablet. The evidence is then stored on an instance of the government cloud and can then be accessed or downloaded via a Callyo website accessible from any DEA computer connected to the Firebird network.[2]

DEA has prepared this Privacy Impact Assessment because Callyo will collect personally identifiable information.

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.

Federal law permits government agents, acting with the consent of a party to a communication, to intercept telephone communications, as well as any oral and other electronic communications without a warrant. 18 U.S.C. § 2511(2)(c), (3)(b). Callyo is a software platform and suite of applications used by law enforcement organizations to record cellular phone conversations with the consent of one of the parties. The system will also permit a body wire application to be associated with a cellular phone for purposes of evidence collection and monitoring of user safety.

---

[1] *Knock and Talk Investigations* are a law enforcement technique where officers approach a residence without a warrant to speak with occupants, request consent to search, or gather information. This method relies on voluntary cooperation and is typically used when there is insufficient evidence for a search warrant, but suspicion of illegal activity exists.

[2] Firebird is an on-premises/cloud hybrid, General Support System (GSS) environment that is the primary enterprise information technology (IT) application infrastructure of the DEA. Firebird provides network infrastructure to host multiple internally connected DEA information systems. The Firebird system infrastructure will be covered by its own Privacy Impact Assessment

DEA primarily uses four Callyo applications (collectively referred to as Callyo). Depending on the scenario for them to be used, Callyo applications will be downloaded to the phones of the consenting party and controlling agent. The applications are:

- A phoneline mirroring application,
- A device monitoring application,
- A body wire mimicking application, and
- A body wire monitoring application.

The phoneline mirroring application allows a user to associate a phone number used by an agent or other consenting individual with the user's phone and to record phone calls and text messages sent to or from that individual's phone number.[3] Any communication made to or from the number will automatically conference in the controlling agent's phone for monitoring.

The device monitoring application provides video, audio, GPS tracking, and team communication capabilities for particular deployments. Agents use the device monitoring application on their phones to monitor the audio, video and location of an associated device. Consent is obtained by the agent when the consenting party initiates the live video feed, and location tracking is used as an officer safety tool. Agents can use this application to monitor communications on an associated device by entering the channel and secured personal identification number. The video and audio evidence are streamed to AWS GovCloud, where they are stored until downloaded by the agent as non-drug evidence.

The other two applications are used in conjunction with concealed microphone technology also known as body wires. The body wire mimicking application allows a cellular phone of a consenting party to act as a body wire microphone. Correspondingly, the body wire monitoring application allows agents or officers associated with the investigation to conference themselves into the system to listen to the oral conversations of the consenting party when the phone is active as a body wire. The body wire monitoring application not only allows the cover team to remotely monitor the body wire transmissions but also track its location.

The types of information that are collected, maintained, used, and disseminated by Callyo include names, phone numbers and in some cases physical location data. (See Section 3.1 below). Personal identifiers are collected for logging and retrieval purposes. Callyo may also collect, maintain, or use text messages and audio communications data pertaining to all individuals involved in the consensual eavesdropping for investigative purposes.

In the process of eavesdropping on different devices and communications, the DEA may collect information pertaining to United States (U.S.) citizens and legal residents as well as non-U.S. persons. Data collected can be from phone recordings and oral conversations, and could include names, phone numbers, emails, etc. Callyo data is housed in AWS GovCloud. In the event that data is collected

[3] The number mirrored is associated by assigning each consenting individual's device a unique phone number, which varies based on the provider (e.g., AT&T, Verizon). Agents provide their own numbers (of government issued cellular phones) so that when the mirrored number is used, a conference-style call is initiated. This allows the agent to monitor the call in real time. All call activity is recorded and stored within the Callyo user account management system associated with the assigned number mirrored and that agent's account.

from non-targets during approved eavesdropping operations, that data can be redacted from materials provided in criminal discovery.

Departmental policies and procedures relating to consensual interceptions of non-telephone (oral) communications govern its use,[4] including that approval must be obtained from appropriate officials within DEA's Investigative Support Section, and the AUSA involved in the investigation. A Department official in the Criminal Division must also approve the technology's use in certain, specific instances.[5] Oversight may also include reviews by the Office of Professional Responsibility and the DEA Office of Chief Counsel where appropriate. Additionally, special agents in the field are typically assigned individual user accounts and manage data under divisional and area of responsibility supervisory oversight

The data flow of Callyo after it captures communications, is transmission via secure web services to specialized DEA evidence repositories in the Cloud. DEA is using controlled storage within Amazon Web Services (AWS) GovCloud for DEA's Callyo data. AWS GovCloud is FedRAMP "High" certified, and the Callyo system itself also is categorized as FIPS199 HIGH. The data will be encrypted at the file level. Callyo data is accessed by DEA personnel from the Callyo Website via a network connection on DEA Firebird infrastructure after the agent accesses the website usinga secure, strong password and multi-factor authentication. That standard procedure is for data on Callyo for each case to be downloaded through an encrypted download process to removable media, such as a thumb drive. This is done for the purpose of litigation and evidentiary presentation.[6] Downloaded removable media is then stored in non-drug evidence storage coded to the investigative file. Data is deleted from the AWS Gov Cloud once the investigation is completed.

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	21 U.S.C. § 878 and 18 U.S.C. § 2511.
Executive Order	
Federal regulation	

[4] See Justice Manual 9-7.301 - Consensual Monitoring; General Use, and 9-7.302 - Consensual Monitoring; Procedures for Lawful, Warrantless Monitoring of Oral Communications. The policy establishes that consensual interceptions need not be made under Title III procedures but that the intercepting agency must maintain internal procedures for supervising, monitoring, and approving all consensual monitoring of oral communications and that approval for consensual monitoring must come from the head of the agency or his or her designee (who must be high-ranking supervisory officials at the headquarters level), or in certain cases from Department of Justice officials.

[5] Intercepts involving a member of Congress, a federal judge, or a high-ranking member of the Executive Branch require approval by at least the Deputy Assistant Attorney General of the Criminal Division or higher official, and intercepts involving high ranking state officials, members of the Diplomatic Corps, or individuals under federal protection or custody requires approval by at least the Director of the Office of Enforcement Operation of the Criminal Division.

[6] Removable media of Callyo recordings are stored in non-drug evidence vaults or lockers, are considered part of the investigative case file within DEA's Concorde Investigative Management Program and Case Tracking System (Concorde-Impact) and are tracked via the Centralized Evidence Registration and Tracking System (CERTS). Concorde-IMPACT and its subsystem CERTS will be covered by a separate Privacy Impact Assessment.

Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	Justice Manual 9-7.301 and 9-7.302 (Consensual Monitoring)

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)*
Name	X	A, B, C, & D	Names of members of the public (USPERs and non-USPERs) will 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 intercepted data and communications by consent of members of the public (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.

(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
Place of birth	X	A, B, C, & D	*
Sex	X	A, B, C, & D	The sex of members of the public (USPERs and non-USPERs)is expected to be collected as part of an investigation; the sex 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	*
Vehicle identifiers	X	A, B, C, & D	*
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) will bem collected specific to an investigation; such information of employees, contractors, and other federal government personnel will also be collectedi.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			

(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
Military status or other information	X	C & D	*
Employment status, history, or similar information	X	C & D	*
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	*
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) are expected to 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	*
Foreign activities	X	C & D	Information related to foreign activities by members of the public (USPERs and non-USPERs) is likely to be collected specific to an investigation.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	*
Juvenile criminal records information	X	C & D	*
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	*
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
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) will be collected specific to an investigation; such information relative to employees, contractors, and other federal government personnel would be collected incidentally.

(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
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, & D	Location information of members of the public (USPERs and non-USPERs) will be collected specific to an investigation if discussed or available; such information of employees, contractors, and other federal government personnel also could be collected.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, & D	Photographs and photographic identifiers, information et of members of the public (USPERs and non-USPERs) are expected to be collected 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) are likely to be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected incidentally.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			

(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
- **Voice recording/signatures**	X	A, B, C, & D	Voice recordings and voice signatures. of members of the public (USPERs and non-USPERs) will be collected specific to an investigation; such information of employees, contractors, and other federal government personnel also could be collected.
- **Scars, marks, tattoos**	X	A, B, C, & D	*
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A & B	System admin/audit related information of relevant employees, contractors, and/or other federal government personnel with access to the system will be collected.
- **User passwords/codes**	X	A & B	See above
- **IP address**	X	A & B	See above
- **Date/time of access**	X	A & B	See above
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible): **Unknown PII**	X	A, B, C, & D	Possible instances of 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 if included in a communication;.

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	X	Email	X		
Other (specify):					

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

Non-government sources:					
Members of the public		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		X	Inside the system, users can only directly access their respective audio/videos via their account, as well as any subordinate's videos as established by group permissions. However, information downloaded from Callyo can be shared intra-agency via removable media or electronic transmission from such media for the purpose of sharing information with associated

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.**
				investigations for criminal intelligence and dissemination of criminal intelligence or litigation.
DOJ Components	X			Via removable media or electronic transmission for the purpose of litigation; potential for criminal intelligence and associated investigations information sharing.
Federal entities	X			Via removable media or electronic transmission from such media for the purpose of litigation and potential for criminal intelligence information sharing under applicable routine uses.
State, local, tribal gov't entities	X			Via removable media or electronic transmission from such media for the purpose of litigation, and potential for criminal intelligence information sharing, under applicable routine uses.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Via removable media or electronic transmission from such media for the purpose of litigation under the appropriate routing uses.
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.

The Callyo suite assists with evidence gathering, personnel and witness security during special investigative operations. Notifying investigative targets of the tool's use in specific instances will undermine the investigation and operational safety. However, the cooperating individual who carries the Callyo associated phone in question has notice that they are carrying the Callyo application, and that it allows the phone to be used as a recording device.

General notice to the public is provided by publishing this PIA, as well as through System of Record Notice (SORN) JUSTICE/DEA-008, *Investigative Reporting and Filing System,* 77 Fed. Reg. 21808 (Apr. 11, 2012) .

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.

There is an established procedure for a Special Agent to follow to conduct a consensual intercept whereby the cooperating party is briefed on their role and what to do and that includes the opportunity to voluntarily participate. After the application is installed on the cooperating individual's phone, the cooperating individual is able to delete the Callyo application from their device at any time through the device's traditional application management capabilities. However, there is no opportunity for the non-consenting party to a conversation with a consenting party to decide to voluntarily participate in DEA's gathering of information via intercept. See answer to 5.1.

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.

Information in Callyo is subject to disclosure in criminal, civil or administrative litigation, consistent with legal requirements. Information contained in JUSTICE/DEA-008, *Investigative Reporting and Filing System*, is exempt from Privacy Act access and amendment requirements, see 28 C.F.R. § 16.98.

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).

	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): Issued December 5. 2022. This system is part of the Ongoing Authorization Program. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:**
X	No current privacy POAMs
	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:
	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: DEA has determined this information falls into the Types "Criminal Investigation and Surveillance Information" and "General Government – Information type PII" in NIST 800-60 because it involves the collection of evidence required to determine responsibility for a crime, the monitoring of cooperating parties' communications, and location tracking of cooperating parties and DEA personnel. The provisional impact level recommended for criminal investigation and surveillance information is MODERATE because the adverse effect on individuals if confidentiality is lost would be serious, as individuals could have publicized their status a cooperating individual or confidential source with the DEA, or as DEA law enforcement personnel associated with the investigation, and/or the DEA itself may suffer the loss of a valuable mode of gaining further relevant investigatory information. Cooperating individuals may suffer reputational harm and embarrassment if the public knew they were the working with DEA in an investigation. Additionally, NIST states the following, regarding special factors that will affect the impact determination for criminal surveillance information: "Information that reveals the identity and/or location of informants may be of particular concern. In such cases, the confidentiality impact level is high." (pg. 181). Therefore, the special factor increasing the sensitivity of the information from a loss of
X	confidentiality in 800-60 and guidance from the Office of Privacy and Civil Liberties

	mandates such designation be HIGH. Accordingly, DEA categorized Callyo as HIGH. DEA has created a POAM "Callyo FIPS 199 Designation-High- Control Assessments" and will assess and review HIGH baseline controls and complete assessments.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** For Callyo, monitoring, testing, and evaluation are conducted as required by NIST are part of ongoing ATO process. Annually, core controls are assessed by the Information System Security Officer (ISSO) with help of the Program Manager/Owner (PMO), technical leads and vendors. (including but not limited, vulnerability patch management, incident response planning and testing, and contingency planning and testing). Since CALLYO has been designated as HIGH, we will follow aggressive timelines for Vulnerability patch management, control re-assessments (making sure HIGH baseline controls are fully tested and assessed annually. The ongoing authorization program that Callyo is under, requires a change control process. DEA's Change Control Board is run through the "ServiceNow" information system, so that system serves as DEA's "trigger log" for system changes. However, because trigger logs are automatically 'pullable' from ServiceNow, they are not entered into the Joint Cybersecurity Authorization Management system (JCAM) but instead, they are tracked in ServiceNow.
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:** As noted, Callyo is part of the Ongoing Authorization Program. Such systems will undergo a thorough security review as required by the authorization process. The program will also be reviewed on an annual basis for any significant new risks to privacy, which would require a new or amended PIA. Annually, Core controls are assessed by the ISSO with help of the PMO, technical leads and vendors. (including but not limited, vulnerability patch management, incidence response planning and testing, and contingency planning and testing) Within the system, Callyo creates an "audit log" for all access to each account and all video viewing and export within that account. These auditing trails can be reviewed at any time by authorized DEA supervisors with the necessary permissions. DEA will work with Callyo to ensure that their administrator access aligns with DEA requirements. DEA's ServiceNow system maintains audit logs of Callyo usage, however, because such "audit logs" are not automatically 'pullable' from ServiceNow, they are not entered into JCAM but reside only in ServiceNow.
	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:

	DEA conducts an initial training for Special Agents on how to use Callyo that includes a section on the importance of safeguarding PII obtained. 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.

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?

a. Physical privacy and security controls

Callyo is housed in the AWS GovCloud which is physically housed in secured locations. The system is accessed by users with unique and attributable accounts and multifactor authentication either on DEA's Firebird network within government controlled facilities or on Firebird compatible mobile devices or laptops through appropriate VPN connections when outside government facilities.

b. Technical privacy and security controls

Numerous processes and security controls have been implemented to protect information systems at DEA, including multi-layered encryption and continuous network monitoring. These processes also include:

- DEA ensures all information in CALLYO is encrypted at rest and in transit and the use of current encryption algorithms and validated cryptographic modules in accordance with NIST guidelines
- DEA privileged users continuously monitor, log, and audit the execution of information system functions to detect misuse and to help reduce the risk from insider threats.
- DEA requires the use of multifactor authentication for employees and contractors in accordance with Government-wide identity management standards, such that computer login restrictions that permit only authorized users access to the data. Data is also protected by permission-based restrictions at both the application interface and the file level.

Additionally, DEA maintains an extensive insider threat unit within the Inspection division the function of which is to assess and prevent insider threats (both intentional and unwitting) by deploying a variety of technical tools to ensure DEA policies protecting PII are being followed.

c. Administrative privacy and security controls

DEA also employs a number of administrative controls to protect Callyo, such as a policy of least privilege at multiple layers - network, system, application, and data so that users have role-based access to only the information and resources that are necessary for a legitimate purpose. The administrative controls applicable to Callyo include:

- Adherence to policy of separation of duties to address the potential for abuse of authorized privileges and help to reduce the risk of malicious activity without collusion;

- Requiring authorized users have access to this data/system using userID/password and multifactor authentication.
- The two types of roles are 'Users' and 'Administrators'. The types of users with access to information within the system are Federal Government employees, detailees (such as Task Force Officers), and contractors. On-site tech personnel will be the designated System Administrators. Users are granted access based upon what the Administrators deem necessary and by what is approved by leadership. By default, Each 'User' only has access to evidence which entered under their log in.

Within the Callyo application, there are two primary user roles: Users and Administrators.

- Users: These accounts are created and assigned by an Administrator. Once set up, the user receives an email or text with a secure link to establish their password and gain access. Each login requires a user ID, password, and multifactor authentication. By design, end users only have access to the evidence they enter under their own login.
- Administrators: Administrators are designated by the divisional administrator and may include staff from a district office or another entity within the divisional area of responsibility. They manage accounts, set permissions, and ensure that all access is consistent with leadership approval. In many cases, on-site technical personnel serve in the Administrator role.
- Direct access to the Callyo system itself is restricted to federal employees, Task Force Officers, and contractors. Inside the system, users can only access their respective audio/videos, via their account as well as any subordinate's videos established by group permissions. Permissions are granted strictly on an operational need-to-know basis, ensuring individuals only have the level of access required to perform their duties. Any local partners would not only receive relevant information extracted from the system.
- Isolation of sensitive or critical information systems, applications, databases, and information into separate security domains with appropriate levels of protection based on the sensitivity or criticality of those resources;
- DEA data-level protections and access controls require individuals within DOJ (including TFOs) have appropriate authorization and need to know, and that the appropriate level of identity proofing or background investigation is conducted prior to granting access;
- To disseminate Callyo information outside DOJ would require identification of an appropriate routine use and documentation of such dissemination to particular parties regarding the particular individual(s) involved on the DEA-381 disclosure form.
- DEA policy is that only individuals with legitimate need for access will have the ability to decrypt sensitive information

Further, in accordance with the DEA Operations Manual for controlled procedures for creating a new employee account, all new account actions on the system must have the written approval of the Program Manager and Section Chief. Account management actions, including the actual assignments of roles and rules, are verified according to established security and auditing procedures. Account management actions are monitored by the System Administration Team on a daily basis to ensure that unauthorized users are not added to the system, or permissions elevated to provide existing users with

unauthorized levels of access. For DEA agents, as well as federal or local law enforcement partners within DEA-led taskforces, access is determined by operational need. Administrators grant and manage access based on leadership approval, and accounts remain active as long as the individual remains in a role that requires use of the system.

Lastly, DEA requires mandatory agency-wide information security and privacy awareness and training programs for all employees and contractors on an annual basis. This includes both computer security training and as of 2025, annual refresher privacy training to protect personally identifiable information.

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.)

Evidence is copied on removable media or electronic transmission as the case is brought to adjudication. The data is downloaded through an encrypted download process to a removable media. This is done for the purpose of litigation and evidentiary presentation. Downloaded removable media is then stored in non-drug evidence storage coded to the investigative file. This is a secure dedicated room with limited access to the inventory and is logged in the room via an inventory system. Data is then deleted from the AWS Gov Cloud once the investigation is completed. But data remains on removable media in non-drug evidence storage areas in DEA field division offices but particularly relevant portions may be transcribed and uploaded to the electronic case file. The removable media recordings are retained consistent with National Archives schedule, Job Number N1–170-04–10 (Sept. 22, 2004).

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?

a. Potential Threats Related to Collection of the Information

Risk: Individuals who are not under suspicion and are not subjects of investigation may be unaware of DEA's collection of their PII and thereby not be able to consent to or otherwise control the collection of their information. This could chill their exercise of 1st amendment activities, due to a loss of their expectation of privacy without regard to whether the individual is actually affiliated with criminal activity.

Mitigation: This risk is partially mitigated. DEA is publishing this PIA to provide some transparency to the public about the data it collects via this system. DEA also provides general notice in the applicable SORN(s). However, the risk of incidental third-party PII collection cannot be mitigated by providing notice of its collection via Callyo without compromising the lawful investigation for which the collection is being undertaken. If information is incidentally obtained about others not involved in a as part of 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. Recordings of entire conversations about unrelated third parties determined to be non-relevant would be deleted from the system and not downloaded onto removable media, though non-relevant portions of an otherwise relevant conversation could be maintained for context and evidentiary reasons.

Callyo is only employed pursuant to an approved investigative activity, which requires approval from a Supervisory Special Agent. However, providing notice to non-suspects whose PII is collected incidentally is not practical as it would run the risk of compromising the collection by potentially tipping off of the suspect, undermining the ability of law enforcement agencies to effectively enforce the law, and could put law enforcement officers at risk. For this reason, notice of collection and the opportunity to consent to specific uses of the data available through systems like Callyo are generally not provided. Further, all data collected by Callyo is obtained for law enforcement purposes in the course of active investigations. Therefore, the notice requirement is exempted by 28 C.F.R. § 16.98 to the extent Callyo data fall within the DEA's Investigative Reporting and Filing System with respect to targets of criminal investigations.

Privacy Risk: DEA may collect more information than is necessary for an investigation or collect information on activities beyond the scope of DEA's Title 21 authority.

Mitigation: This risk is partially mitigated. Every deployment of Callyo occurs during authorized investigative activities which must approved by appropriate supervisory personnel wherein DEA's Title 21 authority and information collection scope issues should be addressed. DEA has implemented policies on consensual monitoring that are modeled on Department of Justice guidance, which impose limits and approval requirements.[7] Use of Callyo must have U.S. Attorney's Office concurrence and DEA Headquarters approval for non-emergency usages, or SAC or their designee's approval for emergency usages, and in some cases of , Department approval from an official in the Criminal Division. The approval is obtained through either of two methods: one for non-emergency

[7] See Justice Manual 9-7.301 - Consensual Monitoring; General Use, and 9-7.302 - Consensual Monitoring; Procedures for Lawful, Warrantless Monitoring of Oral Communications.

circumstances and the other for emergency circumstances. Emergency circumstances are defined as those in which the need arises less than 48 hours before the intended intercept. The name of the concurring Assistant U.S. Attorney is to be documented. In the unlikely event information is collected clearly beyond DEA's Title 21 authority, DEA would redact such information.

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: DEA is using controlled storage within AWS GovCloud for DEA's Callyo data, controlled and managed by a DEA team. Data is encrypted at rest and in transfer using AES 256-bit encryption. Security is also protected during transfer to Callyo/AWS GOV Cloud. The AWS GOV Cloud has achieved Fed RAMP authorization at the High level and Callyo achieved Authority to Operate (ATO) at the moderate impact level , which is a security designation applied to controlled unclassified information across federal government agencies. In data transfers, Callyo also uses AES 256-bit encryption along with AWS KMS (Key Management Service) which encrypts both the data and then encrypts the Data Keys,

In addition, transmitting information from Callyo to AWS GOV Cloud requires a "handshake" (double key) dual authentication with the server any time data is uploaded or retrieved done via an internet or cellular connection.. Further, inside the system, users can only access their respective audio/videos, via their account as well as any subordinate's videos established by group permissions. Each type of evidence is maintained in accordance with its related records retention schedule.

Other technical security measures are in place to safeguard Callyo information within Firebird as well, including: IT monitoring tools; firewalls at the system boundaries; intrusion detection at the systems edge, data loss prevention mechanisms; and audit logs to provide system security.

Administrative access controls also exist. The types of users with access to information within the system are Federal Government employees, detailees and contractors On-site tech personnel will be the designated System Administrators. Only Administrators can make changes to the system, which includes moving or deleting files. The Administrators will give limited system access to agents/officers for making copies and downloading copies to encrypted removable media.

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 Callyo 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. Additionally, Callyo creates an audit log for all access to each account and all video viewing within that account

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 Callyo program.

Mitigation: DEA mitigates these disclosure risks by strict access and dissemination controls. Regarding internal DEA access, DEA uses authentication tools and enforcement of a need-to-know limitation. Callyo requires a Multi-Factor Authenticator (MFA) for users to log in. Additionally, DEA is working to incorporate OKTA[8] as an additional MFA. Callyo does not have a mechanism to share information outside DEA. As such, any sharing occurs via traditional law enforcement sharing mechanisms outside the system. DEA policy mandates that all external (i.e., non-DOJ) dissemination be documented on DEA Form-381 which logs how disseminations are consistent with 28 CFR § 0.103.0, System Of Record Notice routine uses, and other applicable laws and regulations. Further, DEA personnel ensure that the disseminations are shared only with those authorized to receive them for legal and authorized purposes. 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 are the Federal Government and the Task Force Officers.

[8] Okta provides identity and access management solutions that enable organizations to securely implement multi-factor authentication to gain access to their networks and applications. See https://www.okta.com/.