Criminal Division

Privacy Impact Assessment
for the
Legal Process Generators

Issued by:
Jennifer A. H. Hodge
Criminal Division, Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: July 18, 2022

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The United States Department of Justice (Department), Criminal Division (Division) is subdivided into numerous Offices or Sections (hereto forth "Offices") which provide specialized legal expertise, supplemental prosecutorial assistance, and policy guidance on some of the most sensitive and high-profile investigations and prosecutions handled by the Department. The Offices assist Federal, state, local, tribal, and international prosecutors and law enforcement in navigating the increasingly complex landscape of technology-based investigations and prosecutions, in part, by providing resources to simplify and automate the inclusion of provider information for 2703(f)[1] preservation letters, 2703(d)[2] court orders, 2705(b)[3] nondisclosure orders, Electronic Communications Privacy Act[4] (ECPA) subpoenas, and Pen Register and Trap and Trace Device (Pen-Trap) orders[5] (collectively "legal process documents" or "LPDs") to Internet Service Providers (ISPs), wire communication providers, electronic communication providers, crypto-money service businesses (MSBs)[6] and other similar service providers (hereto forth collectively called "providers"). Previously, each LPD was generated manually by the Offices in a resource-consuming effort.

As part of their mission, the Offices develop applications which assist in the generation of LPDs that address specialized requirements specific to their purpose, type of provider, or legal specialty. These applications will be referred to as Legal Process Generators (LPGs). An LPG functions as a combined database and form generator that: (a) provides prosecutors with current information about the thousands of providers, including contact information and the law enforcement policies for each provider; and (b) generates draft LPDs in compliance with current legal standards, using the contained contact information. Generating the draft LPDs using the LPG helps prosecutors and law enforcement more easily comply with the Fourth Amendment to the Constitution, the ECPA, the Pen-Trap Statute, the Federal Rules of Criminal Procedure, and the Budapest Convention, among other legal authorities.

The Division is conducting this Privacy Impact Assessment (PIA) to assess and mitigate the risks to the Personally Identifiable Information (PII) collected when using LPGs, includes, but not limited to, an individual's name, business address, business phone number, and business e-mail.

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

---

[1] 18 U.S.C. § 2703(f).). Generally, a letter to a provider mandating the preservation of specific records for 90 days, pending the issuance of a court order or other legal process.
[2] 18 U.S.C. § 2703(d).). Generally, a court order that compels a provider to provide all information obtainable by subpoena, and all other records relating to a subscriber other than the contents of communications.
[3] 18 U.S.C. § 2705(b).).
[4] 18 U.S.C. § 2701 et seq.
[5] 18 U.S.C. § 3121 et seq.
[6] Money Services Business Definition | FinCEN.gov

previously unknown areas of concern or patterns.

Significant amounts of electronic evidence are obtained using LPDs issued to service providers. These LPDs may require service providers to preserve records in order to allow sufficient time to obtain other necessary legal process, or to produce records from requested accounts such as emails, texts, social media accounts, internet services, financial accounts, or similar individualized records. Provider contact information evolves as quickly as technologies do and identifying the correct contact from a fluid industry often requires significant research and verification. LPGs are designed to assist prosecutors and law enforcement in authoring their LPDs in the most efficient, accurate, and legally compliant fashion. An LPG is entirely electronic and aims to prevent redundant research on the part of prosecutors by maintaining a centralized source with up-to-date information.

LPGs merge the providers' professional contact information for legal service and subject account identifier information, which is provided by the prosecutor or investigator, with pre-authored language associated with each specific process. The LPG places the information into a standardized LPD form, which is designed to meet the current legal requirements for that specific use. Additionally, LPGs provide the prosecutor with any special procedures required by individual providers within the database. A provider's contact information is obtained and updated by designated Office personnel, who verify the information with the provider's publicly available website or contact the providers telephonically or electronically to verify the information. Updates to the standardized LPD forms and special procedures which may be required are made on an ongoing basis as the Office becomes aware of the necessity, and full reviews are conducted annually.

Each LPG is a separate application created to meet the functional needs of a specific Office. Each Office managing an LPG will designate specific employees who have full "read and write" access to the underlying data to fulfill their data maintenance needs as necessary. This is managed and performed through CRMLink.[7] Typically, providers' professional contact information is updated by paralegals, but it can also be updated by investigators, analysts, or attorneys within the Office. The data entered through CRMLink will be used to publish a static web site (LPG) containing that contact information, which will be accessible through DOJNet.[8] Users outside of each Office managing an LPG will have read-only access to that Office's LPG, in order to identify and import needed provider contact data into LPDs. After creating an LPD, Department users may separately incorporate the document into an investigative case file; however, Department users cannot save the document within the LPG and they cannot alter the underlying data in the LPG. Subject account identifier information, which is input into an LPD by a prosecutor or investigator, is never saved within an LPG and will only be retained to the extent it is contained in a generated document and incorporated into a case file. Access to DOJNet is limited to Department employees and those federal law enforcement agencies collaborating with the Department; therefore, there is no public access to the LPGs.

---

[7] CRMlink is the Division's Intranet site, with access regulated through the employee's Personal Identity Verification (PIV) credentials. CRMLink is an application of the Custom Database Application System (CDAS).
[8] DOJNet is the Department-wide Intranet site, available to Department employees and those federal law enforcement agencies reporting to the Department.

Unless they are collaborating with the Department, non-DOJ federal, state, local, tribal, and international law enforcement personnel are not permitted direct access to Division information technologies. However, at the controlling Office's discretion, and upon request and approval, entities can be provided monthly updated listings of providers' professional contact information. Additionally, in specific instances of authorized international cooperation, Office employees can use an LPG to generate LPDs on behalf of an international legal partner agency.

The PII contained in an LPG is the minimal information necessary to operate the system. Information about providers is strictly limited to professional contact information, which is collected for the sole purpose of routing legal process documents to a provider. Some of this information is available through the provider's publicly available websites, while some is collected during annual contact with providers. Additionally, prosecutors may have acquired the contact information of individual providers through their own practical experience and share that information with the Office via listserv emails. Unless otherwise defined in the individual LPG descriptions, LPGs may collect the following information:

- Provider company name and contact information
- Provider legal contact person(s), to include name and/or title
- Provider legal process service address
- Provider law enforcement policies
- Provider emergency contact information
- User audit log information, as described in section 6.1 of this PIA

Additionally, the following information may be input into LPG for the generation of LPDs, but will not be saved to the LPG:

- Subject/defendant information, including name and provider account information.
- Law Enforcement or Prosecutor name, title, and contact information for return of responsive information.

The Division maintains addendums to the Legal Process Generator PIA, with details of each application.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Please see each addendum for any unique authorities relevant to an individual LPG.

Authority	Citation/Reference
Statute	5 U.S.C. § 301; 18 U.S.C. §§ 2510, 2701, 2703(f), 3001 *et seq.*, 3121-3127; 28 U.S.C. § 510, 516, 519; 44 U.S.C. § 3101
Executive Order	Attorney General Directive on Formation of the Cyber-Digital Task Force, February 2018[9]
Federal regulation	28 C.F.R. part 0, subpart K—Criminal Division;

[9] Attorney General Sessions Announces New Cybersecurity Task Force | OPA | Department of Justice

	28 C.F.R. § 0.55. General functions (Criminal Division)
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	Federal Rules of Criminal Procedure;[10] The Attorney General's Guidelines on the Asset Forfeiture Program, July 2018;[11] Asset Forfeiture and Money Laundering Statutes;[12] Office of the Deputy Attorney General's Report on the Cyber-Digital Task Force, July 2018;[13] Justice Manual Title 9: Criminal[14]

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.

Please see each addendum for any unique information elements collected by an individual LPG.

[10] https://www.federalrulesofcriminalprocedure.org/table-of-contents/
[11] https://www.justice.gov/criminal-mlars/file/1123146/download
[12] https://www.justice.gov/criminal-mlars/file/1146911/download
[13] Cyber-Digital Task Force Report (justice.gov), see Page 100
[14] https://www.justice.gov/jm/justice-manual

(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	Office employees with updating responsibilities and legal process contacts for the providers. Subject account identifying information input into LPDs may include subject names but will never be saved to the LPG.
Professional email address	X	A, B, C & D	Office employees with updating responsibilities and legal process contacts for the providers.
Professional phone number	X	C & D	Legal process contacts for the providers.
Professional business address	X	C & D	Legal process contacts for the providers.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			

(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			
Personal mailing address			
Personal e-mail address	X	C & D	Subject account identifying information input into LPDs may include subject email addresses but will never be saved to the LPG.
Personal phone number	X	C & D	Subject account identifying information input into LPDs may include subject phone numbers but will never be saved to the LPG.
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	C & D	Subject account identifying information input into LPDs may include subject financial account information but will never be saved to the LPG.
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			

(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
Legal documents	X	C & D	Legal documents relating to individuals and containing PII will be generated using LPGs but will never be saved to the LPG.
Device identifiers, e.g., mobile devices	X	C & D	Subject account identifying information input into LPDs may include subject device identifiers but will never be saved to the LPG.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			

(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
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	LPGs maintain user activity and audit information.
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	LPGs maintain user activity and audit information.
- **Queries run**			
- **Actions taken within the system**	X	A	LPGs maintain user activity and audit information.
Other (please list the type of info and describe as completely as possible):	X	C & D	Identifying information properly input into LPDs could incidentally include other identifiers, but the contents of individual LPDs will never be saved to the LPG.

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

Please see each addendum for any unique sources of information relevant to an individual LPG.

Directly from individual about whom the information pertains		
☒ In person	☒ Hard copy: mail/fax	☒ Online
☒ Telephone	☒ Email	
☒ Other (specify):	Directly from the provider.	

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

Non-government sources		
☐ Members of the public	☒ Public media, internet	☒ Private sector
☐ Commercial data brokers		
☒ Other (specify):	Directly from the provider's website, or the provider themselves.	

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.

Please see each addendum for any unique information sharing relevant to an individual LPG.

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	☒	☐	☒	Information will be provided to federal prosecutors or law enforcement as needed to generate their legal process documents.
DOJ Components	☒	☐	☒	

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.**
Federal entities	☐	☒	☐	Requesting federal law enforcement agencies are provided with a static list of the Provider contact and special procedure information on a monthly basis.
State, local, tribal gov't entities	☒	☐	☐	Requesting law enforcement agencies are provided with a static list of provider contact and special procedure information on a monthly basis.
Public	☐	☐	☐	
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☒	☐	☐	LPDs generated by LPGs may be used or disclosed during judicial proceedings.
Private sector	☒	☐	☐	LPDs generated by LPGs may be issued to the appropriate provider.
Foreign governments	☐	☐	☐	
Foreign entities	☐	☐	☐	
Other (specify):	☒	☒	☐	Statistical reports may be submitted to officials outside DOJ (e.g., Congress) concerning the Division's caseload, activities, performance, and needs. These reports will not contain identifying information about individuals.

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.

This information will not be released to the public for "Open Data" purposes.

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.

Providers may be given notice of this collection when Office personnel periodically contact them to ensure the accuracy of their contact information.

Individuals, including provider personnel and subjects, are also provided with general notice of the existence of generic case files through the Division SORN CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007) and amended at 82 Fed. Reg. 24155 (May 25, 2017).

Individuals are provided with general notice of the existence of correspondence management through Departmental SORN DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, last published in full at 66 Fed. Reg. 29992 (Jun. 4, 2001) and amended at 82 Fed. Reg. 24147 (May 25, 2017).

Authorized government personnel are provided with specific notice of the collection of certain information to authorize account creation at the time of sign-up and through notices displayed when logging into DOJ information systems. Authorized government personnel are also provided with general notice of the audit logs maintained by this system through DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021).

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.

Providers may voluntarily participate in this collection when Office personnel periodically contact providers to ensure the accuracy of their contact information. In some circumstances, contact information is made publicly available by the provider on a provider's authorized webpage.

Office paralegals and attorneys will comply with the provider point of contact's preference regarding use of their name. DOJ does not inquire whether the points of contact may be required to provide such information as part of their employment with the provider.

Individuals considered subjects or targets of investigation are generally not provided an opportunity to voluntarily participate in the collection, use or dissemination of case information utilized by this system.

Authorized government personnel are generally not provided an opportunity to voluntarily participate in the collection, use or dissemination of the audit logs and user activity maintained by this system.

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.

Providers may request access, amendment, or correction to the professional contact information contained in the LPG when Office personnel periodically contact providers to ensure the accuracy of contact information.

The public may request access to the information by making a Freedom of Information Act request as published on the Division website.[15]

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).

Please see each addendum for any unique privacy and security controls relevant to an individual LPG.

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):** LPG is an application of the Custom Database Application System (CDAS), for which the current ATO expires on October 18, 2022. **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:**
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** As a sub-system of CDAS, LPG has undergone assessments, penetration tests, and vulnerability scans, and is monitored by other means by the CRM Information Systems Security Officer.

[15] https://www.justice.gov/criminal/crm-freedom-information-act

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 Division collects logs according to the DOJ Cybersecurity Standards, which include Operating System, Web, Database and Application logs for every FISMA-applicable system. Auditing controls are applied from the AU (which stands for "audit") family. Logs are correlated into the Justice Enterprise Logging as a Service system. Access to these logs is provided to the Justice Security Operations Center, who provide security analysis and log monitoring for unusual activity based on the algorithms and analysis that they provide. Information Owners or Stewards who select additional audit review requirements per the NIST control selections in their System Security and Privacy Plan and further defined by entries in a Continuous Monitoring Implementation Plan, may have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the business or information owner.
X	**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**.
X	**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:** One-on-one training, specific to this system is conducted for authorized users with read or write access.

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?

All Division systems implement technical security to reduce the risk of compromise to PII. Specifically, certain access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- LPG has a security categorization of Moderate because the loss of confidentiality, integrity, or availability could be expected to have a serious, but not severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, and the Division has selected the applicable security controls for a Moderate baseline.
- The system is accessible by DOJ employees, contractors, and those federal law enforcement agencies collaborating with the Department only, and utilizes tiered, or role-based access commensurate with the end user's official need to access information. Physical access to system servers is controlled through site-specific

controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to perform the job, and is individually verified by PIV card and pin number.

- The system is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- All LPG users must complete the Department's annual Cybersecurity and Awareness Training (CSAT), as well as read and agree to comply with DOJ Information Technology Rules of Behavior. LPG system administrators must complete additional professional training, which includes security training.
- Audit logging is configured, and logs are maintained to help ensure compliance with tiered or role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.

Overall, LPG's defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

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 disposition of records within LPG will conform to processes and procedures established by the Division Records Management Section (RMS) for the disposition of softcopy records.

LPDs generated by investigators or attorneys are not saved or maintained in this system and will be incorporated into investigative case files. Investigative case files within the Division are generally covered under records retention schedule N1-60-88-10, currently available at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0060/n1-060-88-010_sf115.pdf, and are generally destroyed after 10 years. However, case files maintained by other divisions, federal agencies, or entities may be subject to different records retention schedules.

Contact information and specific procedures for providers is referential only and does not meet the criteria for a record requiring preservation. This information is kept up-to-date and is overwritten when more current information is received.

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. ☒ 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:

Records related to CRM correspondence, cases, matters and memoranda, including but not limited to, investigative reports, correspondence to and from CRM, legal papers, evidence, and exhibits, used to provide investigative and litigation information to management in CRM and the Department, courts, and other law enforcement agencies are covered by System of Records Notice (SORN) JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007 and amended at 82 Fed. Reg. 24155 (May 25, 2017).

User accounts, records and audit logs maintained in this system to monitor system activity are covered by JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021).

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.***

Risks identified below were analyzed for all LPG. Please see the Addendum for information specific to each LPG (which applicable).

Please see each addendum for any unique risks or mitigations relevant to an individual LPG.

Privacy Risk: Unauthorized access or misuse of information.

Mitigation: DOJ employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. LPG also implements access monitoring, privacy, and records controls standardized by the NIST Security and Privacy Controls for Federal Information Systems, as defined in

NIST Special Publication 800-53. Access to this system is limited based on a need-to-know and restrictions which limit users to the minimum access needed. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's Personal Identity Verification (PIV) card and pin number for authentication. It also has been evaluated and authorized to operate according to the risk management framework required by FISMA. An audit log is maintained of all user logins and certain user actions. Notification of the monitoring is presented clearly in a banner that must be affirmatively acknowledged when Division users log into their computer.

Additionally, DOJ employees and contractors must complete annual training regarding handling of PII as part of the Department's CSAT, as well as read and agree to comply with DOJ Information Technology Rules of Behavior. This occurs during their orientation upon entering into service with DOJ, and annually thereafter. Additionally, the Offices provide one-on-one training for personnel granted full access to their LPGs. The Division maintains an Account Management Guide and Configuration Management Guide for individual LPG applications.

The IT system assessment is documented in the DOJ CSAM assessment tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no outside access to this system; administrator access is restricted to the few DOJ employees and contractors who administer the program.

Additionally, the LPG is divided into individual applications for further regulation of access based on the minimum information needed principle. In specific instances where outside entities such as state, local, tribal, or international law enforcement or prosecutors may require the services of an LPG, trained Office employees act as a gatekeeper, using the system to assist the outside entity. In such instances, only the gatekeeper can physically access the system, and only after confirming that the requestor is an approved participant, and the request is reviewed for legitimacy and appropriateness. If emergency information must be requested from the provider, the physical response is routed to the requestor, thus preventing unnecessary exposure of the information to the gatekeeper.

Privacy Risk: Over-collection of information.

Mitigation: In order to mitigate these concerns, the Division considered the careful minimization of information collection in the design of LPG. The system solicits and collects the minimum amount of required information through structured data fields to help limit the possibility of over collection. Offices request the least intrusive data reasonable to satisfy the requirements of the legal process documents. The system does not solicit or index particularly sensitive information such as social security numbers (SSNs), dates of birth, Federal Bureau of Investigation Numbers, or Federal Bureau of Prison Numbers. Some of the collected information is professional contact information that is generally available to the public through the providers' public websites, although the LPGs may include contact information (names, email addresses, and direct dial telephone numbers) based on the Offices' personal contact with the providers. Even the collection of a provider POC's name is established by the requirements of the provider; if the provider will allow service of the

legal process document upon an internal office, such as their legal department, instead of an individual, then no name is used for the generation of legal process. However, names, direct dial telephone numbers and direct email address are still collected for a particular provider, to be used in cases of questions, issues, or emergencies.

Other identifiers, such as the name of the subject or defendant listed in the information request, the name of the requesting attorney, and their contact information, are not input into the LPG unless absolutely required to accomplish its purpose. That information is not, unless otherwise documented in the addenda to this PIA, saved in the LPG.

Privacy Risk: Erroneous or inaccurate information.

Mitigation: DOJ works continuously to ensure the accuracy of the information in this system. The PII collected from providers is limited to professional contact information that is generally available in the public realm or is collected directly from the provider by the Office personnel annually. A risk still exists, however, to the efficiency of the ongoing investigations. Here, erroneous or inaccurate information could delay or prevent the receipt of investigative information, or the processing of legal process documents. Through the use of LPG system, the Division has improved the ability to update their records on an ongoing basis. Additionally, the Offices have established a policy of routinely performing full verifications of all contact information at least annually. Finally, a reminder for prosecutors to verify the information prior to use appears at the introduction screen of the applications. Thus, every effort is made to diligently review, verify, and correct this information.

Digital Currency Contact List (DCC) Addendum

Section 1: Executive Summary

Presently, the Division is establishing the Digital Currency Contact List (DCC) Legal Process Generator (LPG).

Section 2: Purpose and Use of the Information Technology[16]

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 Money Laundering and Asset Recovery Section (MLARS), Special Financial Investigations Unit (SFIU) serves as MLARS' experts on complex money laundering and forfeiture investigations. In this capacity, SFIU supplements the resources of prosecutorial and law enforcement partners to conduct complex financial investigations in conjunction with MLARS' litigating units. In 2018, the SFIU initiated the Digital Currency Initiative (DCI),[17] in response to Attorney General Jeff Sessions' directive to initiate a Cyber-Digital Task Force[18] to identify how federal law enforcement could more effectively combat global cyber threats. The DCI provides nationwide investigative and prosecutorial assistance, training, and policy development in digital currency matters, including cryptocurrency investigations.[19]

Many of cryptocurrency's central features – including decentralized operation and control, and, in some cases, a high degree of anonymity – lend it to use in criminal activity. For example, cryptocurrency is increasingly used to buy and sell illegal drugs on the dark web; by drug cartels seeking to launder their profits; by rogue states like Russia, Iran, and North Korea to fund cyber-attacks; and by terrorist organizations to solicit funding and conceal purchases. To assist in the combat of these crimes, the SFIU/MLARS is standing up the DCC. The DCC assists federal and state prosecutors and law enforcement to navigate the complexities of issuing LPDs to crypto-money service businesses (MSBs).[20]

---

[16] All additional aspects of this LPG are appropriately documented within the LPG PIA.
[17] Cyber-Digital Task Force Report (justice.gov), see Page 100
[18] Attorney General Sessions Announces New Cybersecurity Task Force | OPA | Department of Justice
[19] Cryptocurrency refers to a specific type of virtual currency with key characteristics. The vast majority of cryptocurrencies are decentralized, as they lack a central administrator to issue currency and maintain payment ledgers—in other words, there is no central bank. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger that is often referred to as the "blockchain," and a network of peer-to-peer users to maintain an accurate system of payments and receipts. As their name suggests, cryptocurrencies rely on cryptography for security. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object.
[20] Money Services Business Definition | FinCEN.gov

Internet Service Providers list (ISP List) Addendum

Section 1: Executive Summary

Presently, the Division is establishing the Internet Service Providers list (ISP List) Legal Process Generator (LPG).

Section 2: Purpose and Use of the Information Technology[21]

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 Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS also assists federal prosecutors and law enforcement in navigating the increasingly complex landscape of obtaining and using electronic evidence in a wide variety of investigations and prosecutions, in part, by providing resources to automate the generation of Legal Process Documents (LPDs) to Internet Service Providers (ISPs). CCIPS accomplishes this using an LPG named ISPList, which was previously maintained within CCIPS as a Microsoft Access database.

Changing ISPList to an LPG, rather than an Access database, will increase security and privacy protections while centralizing access to the system. The modification will transfer ISPList into to a customized application within Custom Database Applications System (CDAS). This new process will: (a) make it easier and faster for authorized users to access ISPList; (b) allow CCIPS to update the ISPList as soon as new information becomes available; (c) adhere more directly to the Division's established access, auditing log, and security protocols; and (d) transfer the application onto a tested and compliant IT system.

[21] All additional aspects of this individual LPG are appropriately documented within the LPG PIA.