National Security Division

Privacy Impact Assessment
for the
Foreign Agents Registration Act (FARA) System

Issued by:
Jocelyn A. Aqua
Senior Component Official for Privacy
NSD

Approved by: Erika Brown Lee,
Chief Privacy and Civil Liberties Officer,
U.S. Department of Justice

Date approved: June 1, 2016

Blank Page

EXECUTIVE SUMMARY

The National Security Division's Foreign Agents Registration Act (FARA) system (hereinafter referred to as "system") collects, stores, and transmits data about agents of foreign principals, as mandated by the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et* seq. Under the Act, agents of foreign principals register with the U.S. Government and make periodic public disclosure of their relationship with the foreign principal, as well as submit information regarding their activities, receipts, and disbursements in support of those activities. The system then makes this data publicly available so that the U.S. Government and American people are informed of the source of information and the identities of persons attempting to influence U.S. public opinion, policy and laws. This Privacy Impact Assessment was conducted for the system pursuant to the E-Government Act of 2002 because personal, work-related, and political data is collected and disclosed to the public, which may be used to identify and locate an individual.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

FARA is a disclosure statute that requires persons in the United States who are acting as agents of foreign principals, and engaged in certain specified activities, to make periodic public disclosure of their relationship with the foreign principal, as well as disclosure of activities, receipts, and disbursements in support of those activities. The general purpose of the Act is to ensure that the American public and its lawmakers know the source of certain information intended to sway U.S. public opinion, policy, and laws, thereby facilitating informed evaluation of that information by the government and the American people. The FARA Unit of the Counterintelligence and Export Control Section (CES) in the National Security Division (NSD) is responsible for the administration and enforcement of the Act.

The FARA system was developed to assist the FARA Unit in collecting, processing and administering tasks associated with the Act. The system is a major application hosted on the Justice Management Division (JMD) platform and is comprised of three major

functional components: a data management and imaging system, an eFile application, and a public data search application. The FARA Unit uses the data management and imaging system to administer registrations, manage documents and generate reports. The FARA Unit also maintains a Department of Justice (DOJ) file, indexed using a DOJ numbering system, and which contains correspondence, attorney work product, emails, and any other materials relating to a registration or any other matter requiring the establishment of an official file. The FARA Unit uses the eFile application to receive registration documents and filing fees from registrants, and it uses the public data search application to disclose information about the registrants to the public.

The eFile application has an interconnected interface with the Department of Treasury's (DOT) Pay.gov service to process filing fees submitted by registrants via ACH[1] and credit card transactions. Many federal agencies use Pay.gov for processing forms, bills, invoices, or authentication decisions, and any registrant's information submitted to Pay.gov is subject to the same protections as any other end-user.[2] In short, Pay.gov encrypts all financial data, provides privacy notices, and does not give other agencies access to data in the Pay.gov system. The remainder of the FARA system is a standalone application under the control of DOJ. In other words, the repository of registration documents that contain personal and work-related information about foreign agents is not connected to any other database.

The type of information maintained and disseminated by the system includes information submitted by registrants required to register under FARA, some of which is personally identifiable information (PII), and for which 22 U.S.C. § 612 mandates disclosure. This includes the registrant's name, nationality, principal business address, all other business addresses in the U.S. or elsewhere, and any residential addresses. If the registrant is a partnership, corporation or other organization, then the registrant must submit the above PII for all of the organization's partners, directors, officers, and anyone performing functions of a director or officer. The Act also requires a statement describing the nature of the registrant's business, the registrant's employees' names, and the name and address of every foreign principal for whom the registrant is acting or has agreed to act.

The Act requires information about the registrant's relationship with the foreign principal. This includes copies of every written agreement, as well as the terms of any oral agreements, that the registrant has made with the foreign principal; the nature and amount of contributions, income, money or thing of value the registrant has received from, or given to, foreign principals; detailed statements of the registrant's activities performed on behalf of the foreign principal; and any other information pertinent to the purpose of FARA.

---

[1] The Payflow ACH (Automated Clearing House) Payment Service facilitates electronic collect payments from customers for either single-entry or recurring payments by directly debiting a customer's checking or saving accounts.

[2] Such privacy protections are addressed in the Financial Management System (Pay.gov) Privacy Impact Assessment 2.0, and available at https://www.fiscal.treasury.gov/fsreports/rpt/fspia/paygov_pia.pdf.

Most information is transmitted into the system by registrants through an electronic filing system. Registrants receive an account number and temporary password by mail to establish their online account. Then, through their online account, registrants upload to the FARA eFile application their registration package of all required documents and pay filing fees. After submission, FARA staff receives and processes all filings and payments, which includes document scan, quality control and review, data entry, fee application, and internal assignments. Documents are stored in the database and uploaded daily to the FARA website for public disclosure through the document search and quick search tools at www.fara.gov. Electronic registration documents are submitted over the Internet using secure hypertext transfer protocol (HTTPS). The information is then transmitted internally through the Justice Unified Telecommunications Network (JUTNET). If a person files electronically, they do not need to file a paper version; however, the FARA Unit receives some registration filings in paper form, including filing fee payments, which are often mailed or delivered in person. In these situations, FARA Unit personnel scan the filings into the data imaging system. Finally, on occasion, when registrants are having difficulties with the electronic filing system, they may receive permission to email registration documents to FARA Unit personnel and mail or hand deliver registration filing fees. Software will scan such emails for malicious components.

The public has access to registration statements, short-form registration statements, supplemental statements, exhibits, amendments, and copies of informational materials or other documents or information filed with the DOJ. The documents are reviewed, and redacted if necessary, when PII, such as date of birth, is inadvertently provided in the registration. The FARA Unit will redact all PII, as defined by the National Institute of Standards and Technology Special Publication 800-122 (NIST 800-122), unless the statute explicitly requires such PII to be disclosed. Thus, the public has access to all registration filings after the documents have been subject, when necessary, to a redaction process.

The public can retrieve information from the FARA system in person or through the FARA website public data search application. For in person retrieval, the FARA Unit maintains a public office on the First Floor of the Bicentennial Building, 600 E Street, NW, Washington, DC 20004, and is open for the public to review the public records from 11:00am to 3:00pm, Monday through Friday. The public data search application is searchable and sortable by certain categories of information, including name of registrant, name of foreign principal represented, date of filing, and registration status. The FARA Unit personnel assist the public with viewing and copying public records; however, they will not discuss pending, potential, or hypothetical investigations, matters or cases with the public. The FARA Unit will not release any information beyond what the statute mandates. Thus, the public does not have access to any other information acquired by the FARA Unit related to registrants such as the information contained in the Department's internal file, which includes correspondence, attorney work product, emails, and any other materials relating to a registration or any other matter requiring the establishment of an official file. Therefore, any other requests for information must be made under the Privacy Act of 1974 and/or the Freedom of Information Act (FOIA). All media requests are referred to NSD Public Affairs.

For online access to the information, the public may access the FARA website, www.fara.gov. The information in the FARA system is directly transmitted over the Internet, using secure hypertext transfer protocol, to the front end of the fara.gov website. The public can search registrants by categories such as registrant number, registrant name, and stamped/received date. Searches can be narrowed by document type (including registration statement, supplemental statement, exhibit, conflict provision, or dissemination report) or status (terminated or active). After a search is conducted online, a public user will have the registration number, name, alias, "doing business as" name, status, registration date, termination date, stamped/recorded date for every registrant within the public user's query, and foreign principal client. For older registrants, there is a notification that the registrant's full registration statement and other documents are accessible at the FARA Unit office, but for newer registrants, there is a link to a scanned copy of the registration documents.

Other parts of the government receive information stored in the FARA system. First, as previously referenced, DOT receives invoice information to process filing fee payments through Pay.gov. Second, as mandated by the statute, the FARA Unit sends monthly updates of publicly available registration documents to the Department of State, filed under FARA. This information is provided on a CD. Additionally, the FARA Unit periodically provides other government agencies requesting the public filings with a CD of the information requested as authorized. Only the NSD IT Staff and the FARA Unit have direct access to the internal FARA system and the documents that are not publicly available registration statements filed under FARA.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify): The FARA Unit uses registration numbers, pay.gov transaction numbers, and 149 DOJ file numbers and IQ (a correspondence tracking tool) numbers used within NSD and not discussed herein.					

General personal data					
Name	X	Date of birth		Religion	
Maiden name	X	Place of birth		Financial info	
Alias	X	Home address	X	Medical information	

General personal data					
Gender		Telephone number		Military service	
Age	X	Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): Birth Year, Nationality, Country of Citizenship – FARA short form registration statements request year of birth for identification purposes.					

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address		Work history	
Work address	X	Business associates			
Other work-related data (specify): Copies of every written agreement, as well as the terms of any oral agreements that the registrant has made with a foreign principal; nature of registrant's business and business activities; names of employees and the nature of their work.					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): None.					

System admin/audit data					
User ID		Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)
Contributions to and from foreign principles
Contributions to political organizations
Other statements, information, or documents pertinent to the purposes of FARA that the Attorney General, having due regard for the national security and public interest, may require.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		

Directly from individual about whom the information pertains
Other (specify):

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal		Foreign		The data management and imaging system and miscellaneous files contain information from many different sources, including the Department of Treausury.	
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

First, there is a risk of unauthorized disclosure of registrants' PII because registrants may inadvertently include sensitive PII in their registration even when it is not requested. For example, registrants may include a document that states their full date of birth (as opposed to only their year of birth), bank account number, or social security number. The disclosure of such information, including year of birth, is not mandated by the statute and, potentially, could pose a significant threat to registrants' privacy. To prevent any unauthorized disclosure of such information, the FARA Unit redacts PII, whether it belongs to registrants, foreign principals, or third parties, unless it is PII for which the Act mandates disclosure.[3] According to NIST 800-122, PII is any information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, as well as information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Thus, the FARA Unit redacts any personal identification number such as a social security number, financial account information, photographic image, or date of birth. The Unit would not, however, redact PII such as name, alias, address, year of birth, or employment information, as this information is mandated by

[3] Although redaction is currently being conducted manually, NSD intends to accomplish this electronically by the end of 2016.

the statute. The Unit collects and discloses the least amount of PII it can while still complying with the statutory mandate.

Second, even if there is no unauthorized disclosure of PII, the amount of PII that must be disclosed to comply with the statute is itself a potential threat to registrants' privacy. The system discloses details of registrants' employment situation as well as their residential addresses. However, registrants could have decided not to serve as an agent of a foreign principal within the U.S., in which case they would not have to disclose any PII. Their decision to be a foreign agent serves as some level of consent that at least mitigates any potential privacy violations.

The system further mitigates privacy risks by only storing information provided by registrants themselves. Though this measure does not prevent public access to the information, it does ensure that registrants know what personal information is being disclosed to the public and in what manner. Registrants also have the opportunity to update their information to ensure accuracy. This measure safeguards against disclosure of inaccurate information about registrants that could negatively affect their personal or professional lives.

Additionally, the Office of Management and Budget and DOJ policy directives, as well as the Federal Information Security Management Act of 2002, have suggested or imposed limits on the disclosure of residential addresses. Therefore, although the statute requires the disclosure of registrants' residential addresses, the FARA Unit has adopted select limits on how those residential addresses are disclosed broader than the statutory requirements. When the FARA Unit receives a request, with justification for redacting from registration forms appearing on the FARA website PII required to be disclosed under FARA (*e.g.*, residence addresses), the FARA Unit will redact the information and maintain an unredacted version in the FARA files. Any person dissatisfied with the redacted web version can come to FARA's public office during business hours to receive an un-redacted version of the registrant's statement.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): The information collected and stored in the system is to ensure that the U.S. Government and the people of the U.S. are informed of the source of information (propaganda) and the identity of persons attempting to influence U.S. public opinion, policy, and laws. However, because the registrant documents are public, there is no limit on how the information is used. Thus, the information may serve additional secondary purposes.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Post-World War II era, foreign governments and corporations sought to influence U.S. foreign and domestic policy agendas and began hiring political consultants and law firms to promote their own economic and political interests. The purpose of FARA is to ensure that the American public and its lawmakers know the source of certain information intended to sway U.S. public opinion, policy, and laws, thereby facilitating informed evaluation of that information by the U.S. Government and the American people.

The FARA system achieves this purpose by initially registering foreign agents and making public their registration statements and supplements. The system provides the public with access to the names of agents engaged in specified activities within the U.S. on behalf of foreign principals, as well as information regarding the foreign principals they represent and the nature of their business relationship. With this information easily accessible, individuals and the U.S. Government can quickly identify whose interests an individual or company is representing.

Finally, the FARA system also serves the purpose of fulfilling a statutory mandate. Each piece of PII collected by the system is necessary to satisfy the statutory requirements of the Act. The registration documents and supplemental information filed are explicitly required by section 612(a). The administrative system also collects IP addresses and time of filing when individuals register through the eFile system. The time of filing is collected so that the FARA Unit can ensure compliance with the statute's filing deadlines and compliance with electronic signature protocols.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	Federal Agents Registration Act of 1938, 22 U.S.C. § 611 *et seq.*
	Executive Order	
X	Federal Regulation	Title 28 C.F.R. Part 5
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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.

FARA records are retained and disposed of in accordance with a schedule proposed by the Department of Justice and approved by the National Archives and Records Administration (NARA). FARA registration records have been appraised by NARA as permanently valuable with a thirty year retention by the Department. (Thirty years after termination of registration, the documents are transferred to the National Archives). The data in the FARA system has also been appraised as

permanently valuable and will be transferred to NARA thirty years after termination of a registration.[4]

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Although there is a potential threat to privacy that could result from unauthorized access to the FARA system, which includes documents that are unredacted, direct access to the FARA database is limited to authorized personnel with the requisite background investigation and security clearance, formal authorization, and a need-to-know. Only limited workstations have access to the document management and imaging system within the FARA system and there is strong password-controlled access to the server from these workstations. Printed documents and digital media are stored in file cabinets and are protected within secured offices during off-duty hours. In addition, servers, workstations, and offices are located in controlled-access buildings. Automated mechanisms such as access card readers are employed to ensure only authorized users have access to the DOJ facility and to the suites where records are stored. In other words, direct access to the FARA system where documents are received is strictly limited and physically secured.

Second, any potential risk that FARA Unit staff access and misuse highly sensitive information disclosed in registrant documents is mitigated through approved NSD IT security practices. NSD enforces the DOJ Information Technology Security Staff (ITSS) Information Technology Security Council Information Technology Security Employee Services (ISES) Training Plan for FARA government staff and contractor personnel. The NSD program follows DOJ internal policy and procedures for sanctions. User non-compliance to security policies and procedures is subject to supervisory disciplinary action up to, and including, immediate termination. Moreover, there are monitoring and auditing tools to review user activity, so the FARA Unit will be able to identify any unauthorized user activity.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components	X			

[4] *See* approved disposition authorities N1-060-88-10, item 149 and N1-060-08-024.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Federal entities		x		Monthly data on CD to Department of State (redacted and unredacted registration documents). Other agencies on a case-by-case basis as requested.
State, local, tribal gov't entities				
Public				Online or in-person access (redacted and unredacted registration documents).
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Unauthorized physical access to FARA data within the hosting facility is prevented through the use of guards, access badge security, sign-in logs, and security cameras, as well as via the implementation of policies and procedures that describe access requirements. Unauthorized logical access to the FARA system itself is addressed by network intrusion detection systems, firewall log monitoring, and malware detection and correction software.

Data is protected through compliance with DOJ access control policy, role-based access control for user identification/authentication, assigning and enforcing authorizations, establishing thresholds, applying information flow restrictions, automated system notifications, session termination, applying the principles of least privilege coupled with need-to-know, and using Department-approved encryption technology for data in transit.

Finally, FARA has established and implemented an account management process to include account justification, requirement of a background investigation and clearance, access restrictions based upon separation of duties and least privilege, strong authenticator management, re-certification efforts, and audit management. *See* also sections 2.3 and 3.5 for additional information.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Pursuant to federal regulation, individuals do not have an opportunity or right to decline providing the information required by the Foreign Agents Registration Act of 1938.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Pursuant to the FARA , individuals do not have an opportunity to consent to particular uses of the information. Moreover, any restrictions on use would be difficult to enforce because the information is publicly available.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Under the Act, the individuals do not have an opportunity or right to decline providing the information or the opportunity to consent to particular uses of the information. Individuals consent by agreeing to work as an agent of a foreign principal. Every registration statement, short-form

registration statement, supplemental statement, exhibit, amendment, or copy of informational materials filed with the Attorney General under this Act is a public record open to public examination, inspection and copying during the posted business hours of the FARA Public Office in Washington, DC or available online at www.fara.gov. Individuals who do not comply or who provide false information may be fined not more than $10,000 or imprisoned for not more than five years, or both. And an alien convicted of a violation, or conspiracy to violate the statutory requirements of FARA, may be subject to removal pursuant to chapter 4 of Title II of the Immigration and Nationality Act, 8 U.S.C. § 1221 *et seq.*

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: [7/27/2015] If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date: [Recertification 7/27/2018]	
X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. System Security Plan for Foreign Agents Registration Act System, July 24, 2015, lists all management, operational, and technical security controls for the FARA system in detail (see pages 18-97). Security plan presents existing and planned controls for ensuring FARA system operates in accordance with applicable laws.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. NSD monitors the FARA security controls on an ongoing basis. Assessment results, including changes to or deficiencies in the operation of security controls are analyzed for impact and documented directly into the Computer Security and Access Management system (CSAM). Changes are made to the SSP and POA&M as appropriate when there are changes to or deficiencies in the operation of security controls. In addition, FARA servers are monitored with a program that provides near real-time reporting to authorized individuals of the security status of the FARA servers.	
X	Contractors who have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors who have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	Other (specify): Security Awareness Training is provided to all FARA administrators and users on an annual basis. PII is addressed in this training.

Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

FARA data in all forms will be protected in accordance with applicable DOJ and Federal guidance, policies, and directives, based on the sensitivity of the information. Access to information is limited to authorized personnel with a requisite background investigation/security clearance, formal authorization, and need-to-know.

FARA mitigates unauthorized disclosure risks through establishing appropriate roles for users, establishing strong authentication mechanisms, executing an annual re-certification, and implementing audit mechanisms. Controls are validated throughout the C&A lifecycle and as risks are identified; they are mitigated via Plans of Actions and Milestones (POAM). In general, FARA information is protected by management, technical, and operational safeguards appropriate to the sensitivity of the information. Users are properly trained in safeguarding identifying information stored within and/or processed by FARA.

The FARA public data search and efiling system limits data collection and data input to scanning documents provided by registered agents. The FARA Unit data imaging system collects registration filings, correspondence, and other materials received in connection with administration of the statute. NSD provides government staff and assigned contractor personnel mandated privacy training on the use and disclosure of personal data. NSD follows ITSS procedures and policies to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuse.

NSD considered the risks to the system and the sensitivity of the data as a basis for selecting security safeguards to provide adequate system protection. The system provides the capability to securely authenticate users before allowing access to system resources, disables inactive sessions within a specified time period, and provides the capability to audit system activity.
During system identification and authentication, the authenticator field is masked with asterisks. *See* section 4.2 for additional information.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: System name: Registration and Informational Material Files Under the Foreign Agents Registration Act of 1938 SORN number: JUSTICE/NSD-002, 72 FR 26153.

	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Many FARA registrants are U.S. citizens or lawfully admitted permanent resident aliens, so the description in section 2.3 of how information in the FARA system is retrieved and then accessed applies to all persons. The FARA system's privacy protections do not differ depending on whether the registrant is a U.S. person. Information is self-reported and submitted through the eFile system, by mail, in person, or via email, and registrants are mandated by law to provide this information regardless of nationality.