United States Department of Justice (DOJ)
Office of Privacy and Civil Liberties (OPCL)

Office of Justice Program

Privacy Impact Assessment
for the
Denial of Federal Benefits and Defense Procurement Fraud Debarment Clearinghouse (DFB/DPFD)

Issued by:
Maureen Henneberg

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: [February 16, 2023]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Office of Justice Programs' (OJP) Bureau of Justice Assistance (BJA) is responsible for receiving, maintaining and responding to inquiries from Federal agencies, contractors, or subcontractors regarding debarments pursuant to the Denial of Federal Benefits (DFB) and Defense Procurement Fraud Debarments (DPFD) program. Individuals listed on the debarment list are generally precluded from receiving federal benefits. BJA receives information on qualifying drug cases from federal and state courts, and qualifying Department of Defense (DOD)-related cases from Department of Justice (DOJ) litigating divisions and enters it into DFB/DPFD. BJA transmits the information contained within DFB/DPFD to the System for Award Management (SAM), a General Services Administration (GSA) system that consolidates eight Federal Procurement Systems, including the system known as the Excluded Parties Listing System (EPLS). All federal agencies are required to consult the GSA publication "List of Parties Excluded from Federal Procurement and Nonprocurement Programs," more commonly known as the "Debarment List," to ensure statutory compliance when awarding federal funds. Debarment actions are also communicated to all government agencies through the SAM. Exclusions pursuant to DFB are also provided directly to the Department of Education (ED) and the Federal Communications Commission (FCC).

Pursuant to the requirements of privacy provisions under the E-Government Act and OMB's M-03-22 implementation guidance and in congruence with the DOJ/OJP standards and procedures a Privacy Impact Assessment (PIA) is deemed necessary due to the nature of the data being collected, stored, and maintained in DFB/DPFD. At a high level, the information system stores an individual's personal information, Social Security Numbers (SSNs), legal and criminal information, Federal identifiers, as well as the name and signature of the sentencing judge. SSNs are given special protection and those protections are elaborated on in Section 6 of this PIA. This PIA will outline the types of data and information collected, maintained and disseminated along with the privacy and security controls in place to secure any PII.

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.

Under 21 U.S.C. § 862, the Attorney General delegated the administration of the DFB program to the OJP. Later, as directed under 10 U.S.C. § 2408, the Attorney General became the Single Point of Contact for a defense contractor or subcontractor to promptly obtain information regarding whether a person that the contractor or subcontractor proposes to employ has been convicted of defense-contract related felonies and/or related criminal penalties imposed on defense contractors. The establishment of this repository, known as DPFD program was also assigned to OJP. Today, the BJA maintains the two, legally distinct, clearinghouses as a single point of contact, which follow a single set of policies and procedures to receive, maintain and provide information for both types of qualifying debarment cases.

Specifically, debarment under the DFB program precludes an individual convicted of trafficking in or possession of drugs from receiving all or selected federal benefits. 21 U.S.C. § 862 (d) (1) defines "federal benefit" as "…the issuance of any grant, contract, loan, professional license, or commercial license provided by an agency of the United States or by appropriated funds of the United States." And, 21 U.S.C. § 862 (d) (2) states that the definition "…does not include any retirement, welfare, Social Security, health, disability, veterans benefit, public housing, or other similar benefit, or any other benefit for which payments or services are required for eligibility."

The DPFD program maintains a database of those with a fraud or felony conviction(s) arising out of a contract with the DOD. Such conviction prohibits an individual from being involved with a defense contract or first-tier subcontract of a defense contract. Federal Acquisition Regulation Subpart 22.801 defines a first-tier subcontractor as a subcontractor holding a subcontract awarded directly by a Federal government prime contractor.

The two clearinghouse programs are commonly referred to as the "Denial of Federal Benefits" program.

BJA is responsible for receiving, maintaining, and responding to inquiries from Federal agencies, contractors, or subcontractors regarding debarments pursuant to the aforementioned laws. Qualifying drug cases are submitted by federal and state courts. Qualifying DOD-related cases are submitted by DOJ litigating divisions. Information contained within the clearinghouse databases must also be transmitted into the SAM, a GSA system that consolidates eight Federal Procurement Systems, including the system known as the EPLS. Debarment actions are communicated to all government agencies through the SAM, at https:///www.sam.gov. The DFB clearinghouse database records regarding exclusions pursuant to DFB must also be provided directly to the ED and the FCC. All federal agencies are required to consult the GSA publication "List of Parties Excluded from Federal Procurement and Nonprocurement Programs," more commonly known as the "Debarment List," to ensure statutory compliance when awarding federal funds.

DFB/DPFD generates reports on active debarment cases in XML format that are specific to GSA (SAM), ED, and FCC. DFB/DPFD sends monthly reports to GSA and FCC. All Personally Idenfitifiable Information (PII) is encrypted using 256-Bit AES encryption.

Data is shared with the GSA (SAM), FCC, and ED. SAM provides a single list of individuals and firms excluded from Federal assistance. DFB/DPFD Clearinghouse personnel generate monthly updates to GSA. These same personnel log in to GSA's website and upload the data from DFB/DPFD to GSA. Similar to the process with GSA, DFB/DPFD Clearinghouse personnel generate a specialized report for the FCC during the first week of the month from DFB/DPFD, encrypt it, and email the encrypted file to a specific FCC email address. Authorized personnel at the ED have an approved DFB/DPFD account. This authorized personnel logs in monthly to generate a specific ED report. The ED personnel are connected to the DFB/DPFD system though HTTPS. Data is encypted and the authorized user must go through an approval and authentication process before gaining system roles-based access to DFB/DPFD.

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
X	Statute	DFB was established under Section 5301 of the Anti-Drug Abuse Act of 1988 (Public law 100-690; 21 U.S.C. § 862). DPFD was established under Section 815, Subsection 10 of the National Defense Authorization Act (Public Law 102-484; 10 U.S.C. § 2408).
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

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	C and D	Full name of members of the public who are denied federal benefits, and sentencing judges.

(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
Date of birth or age	X	C and D	DOB of offender provided by the court.
Place of birth			
Gender	X	C and D	Sex of offender provided by the court.
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Full SSN of offender provided by the court.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C and D	Address of the offender provided by the court.
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
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			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	The following information is collected on the offender and includes information related to criminal

(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
			prosecution: date of sentence, case or docket numbers of court cases, drug trafficking or possession conviction, terms of sentence under statute, potential indication whether drug treatment or community service required, name of sentencing judge, duration of denial of federal benefits, which benefits are denied, all prior drug offenses with case numbers, date federal benefits restored by action of the court, signature of sentencing judge, name of sentencing court.
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	X	A and B	Email and username are collected for authorized OJP employees and contractors; judicial participants; and agency users.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			

(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
- **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:	X	A and B	User ID and audit data are logged to meet system auditing requirements from DOJ security controls.
- **User ID**	X	A and B	
- **User passwords/codes**	X	A and B	
- **IP address**	X	A and B	
- **Date/time of access**	X	A and B	
- **Queries run**	X	A and B	
- **Content of files accessed/reviewed**	X	A and B	
- **Contents of files**	X	A and B	
Other (please list the type of info and describe as completely as possible):			

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		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal Entities	X

Government sources:					
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Information on drug-related offenders is obtained from the clerks of the relevant federal and state courts. Information on qualifying DOD-related cases are submitted by DOJ litigating divisions.					

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	The Program Manager, Administrator and System Administrator can search/view existing case and offender information.
DOJ Components				
Federal entities	X		X	Federal agencies that award/provide Federal benefits can access individual verification requests that they have submitted.

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.**
				Agency users in GSA, FCC, and ED with Agency role can generate an XML file with PII on active cases. DFB/DPFD securely sends monthly reports to GSA and FCC. Authorized ED personnel log in to DFB/DPFD monthly to generate a specific ED report. Information is disseminated and used to validate Data Universal Numbering System (DUNS) numbers and Unique Entity Identifiers (UEI), which are used to identify businesses, through the use of SAM.gov.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X		X	Judicial participants (court users of DFB-DPFD, generally clerks of the relevant federal and state courts) can search/view existing case and offender information only as submitted by their respective courts.
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.

A Federal Register System of Records Notice (SORN) for the Denial of Federal Benefits Clearinghouse is available for members of the public to access at:

- 64 FR 25071 (5-10-1999)*
- 66 FR 8425 (1-31-2001)
- 82 FR 24147 (5-25-2017)

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.

Individuals will not have the option to opt out of the collection, use, or dissemination of information in the system. The information in the clearinghouse is submitted by federal and state courts, and DOJ litigating divisions. The information is used to compile the Debarment List which identifies individuals excluded from receiving Federal benefits.

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

An individual may request access to a record pertaining to them, or request amendment to their record, by submitting a written request to the DFB/DPFD System Manager. Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "Record Access Procedures" paragraph in the SORN. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls**

	and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): 06/24/2020-06/24/2023 **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 part of the monthly continuous monitoring process, and the system authorization and assessment life cycle, applicable security controls are monitored, tested, and evaluated. Any weaknesses identified are captured appropriately within a POA&M. In addition, OCIO has been monitoring and tracking the known vulnerabilities for the system under the OMB MAX FedRAMP Continuous Monitoring. In addition, DOJ/OJP monitors the monthly continuous monitoring submissions from Cloud Service Providers (CSPs) for all Cloud Service Offerings (CSOs) supporting DFB in accordance with FedRAMP Continuous Monitoring requirements.
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:** All system audit logs are tailored off Splunk. Based on criteria set by the OJP Information Technology Service Division (ITSD), potential exception conditions are distributed to the System Owner, the DFB Technical Support Lead and members of ITSD staff. These 'alerts' are emailed in real time and reviewed as they are received (no less than daily). In accordance with the NIST Special Publication 800-53 control AU-06 (Audit Record Review, Analysis, and Reporting), ITSD Security reviews and analyzes information system audit records weekly and reports findings.
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**.
	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: No additional privacy-related training is required for this system.

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?

DFB/DPFD uses technical controls through role-based privileges to limit users' access privileges. The system implements the principle of least privilege to ensure that only authorized internal users have access to sensitive data. Additionally, these authorized internal users must sign the Rules of Behavior before being granted system access. DFB/DPFD features user identification and password access controls. Accounts are provisioned to a single users and accounts are reviewed by System Administrators on a weekly basis. System Administrators leverage the DOJ Strong Authentication Policy and two-factor authentication is required for remote access.

The system encrypts all SSNs stored in the database (data at rest). Only authorized users can decrypt and view SSNs by virtue of the role-based access privileges of the application. Authorized users include the DFB/DPFD Administrator, the DFB/DPFD System Administrator, the DFB/DPFD Program Manager, and any court users (Judicial Participants) and Agency Users (e.g., ED) that have accounts in the system. Judicial Participants are only able to see cases that are entered by their own courts.

Internally, event logs are stored in the system and/or off the system for audit in accordance with DOJ standards. Audit trails are maintained and system login information is captured. All logs are reviewed at least weekly and archived audit logs are stored offline in an encrypted format for six months. Information is encrypted at rest and in transit within the DFB/DPFD system. Additionally, the information system is categorized as Moderate. The FIPS security categorization of the system matches the security categorization of the most sensitive information in the system, as per the "high water mark" standard.

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.)

BJA must retain all case and offender records. Hard copy records can be destroyed once they are saved in electronic format and can be searched by a unique identifier. The electronic data is maintained in the DFB/DPFD system. Audit logs are recorded and retained in accordance with the National Archives and Records Administration, General Records Schedule, Section 3.2: Information Systems Security Records. Audit trail logs are maintained online for at least 90 days, log rotate is used to retain audit logs, and archived audit logs are stored offline in an encrypted format for at least one year.

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:***

JUSTICE/OJP-013, Denial of Federal Benefits Clearinghouse System (DEBAR)

- 64 FR 25071 (5-10-1999)*
- 66 FR 8425 (1-31-2001)
- 82 FR 24147 (5-25-2017)

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?

Since DFB/DPFD does not collect information directly from individuals, there is a risk that those individuals may not be aware of the collection of their information in the system or that the information may be inaccurate or out-of-date. The DFB Clearinghouse does not control whether courts and/or the DOJ litigating divisions provide notice to the convicted individuals. The DFB Clearinghouse also does not send a notification to individuals that are on the list. In order to mitigate these risks, OJP has published a SORN to provide generalized notice to the public, which includes procedures for individuals to access and amend their records (although some exemptions may apply). Additionally, the relevant courts and litigating divisions notify the DFB Clearinghouse of any updates on the information pertaining to the convicted individuals.

There is a risk of unauthorized access and dissemination when data is transferred between systems and agencies. In order to mitigate this, all PII in DFB/DPFD is encrypted in flight when transferred between the different agencies (GSA, FCC, and ED) using 256-Bit AES encryption. A Memorandum of Understanding (MOU) exists between DOJ and the FCC and a Computer Matching Agreement exists between DOJ and ED. Additionally, an agency role has been created for each Agency so that the Agency user can generate the reports on their own through the system. However, only ED utilizes this role.

The DFB/DPFD system uses a variety of security controls to mitigate the risk of unauthorized access to the system. The DFB/DPFD system is monitored by the System Administrative User. Each User has a unique username and is assigned a role. Application user registration is approved by the System Administrative User. The server only uses SSH secure connection and the DFB System Administrator User monitors all the ports that run on the server daily. Two-factor authentication is used for remote access and users must first connect to VDI to access the application. In accordance with OJP OCIO 30: Account Management, stagnant accounts are deactivated after 90 days. When logging in, passwords are obscured with dots. The DFB/DPFD system uses open SSL cryptographic modules used for both HTTPS and SSH encryption.