Office of the Inspector General

Privacy Impact Assessment Addendum
for the
Inspector General Network for Telecommunication and Exchange (IGNITE) System: OIG Data Analytics Program

Issued by:
William Blier, OIG Senior Component Official for Privacy

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [July 16, 2018]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The United States Department of Justice (DOJ or Department), Office of the Inspector General (OIG), employs a general support system entitled the Inspector General Network for Information and Technology Exchange (IGNITE) System. The primary functions of this system include, but are not limited to, e-mail, word processing, spreadsheet, presentation, project management, file and printer sharing, and access and storage to databases and minor applications utilized for the OIG to effectively carry out its mission to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel.

In order to carry out these functions, the IGNITE System will need to store, process, and transmit personally identifiable information (PII). The IGNITE System Privacy Impact Assessment (PIA) was published on January 18, 2017.[1] The OIG Data Analytics Program (DA Program) will be managed within the IGNITE System boundary. The integration of the Data Analytics Program will add more records containing PII, collected from sources other than those indicated in the IGNITE System PIA, for the purposes described below. As a result, this PIA Addendum to the IGNITE System PIA has been prepared.[2]

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:

> The OIG is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in DOJ programs and personnel, and to promote economy and efficiency in those programs. The DA Program is being implemented to assist with the performance of OIG audits, investigations, and reviews, and to accommodate the requirements of the Digital Accountability and Transparency Act of 2014 (DATA Act). The DA Program will allow the OIG to analyze large volumes of data, thereby helping the OIG to effectively orient its efforts to areas of identifiable risk, and enhancing its ability to perform its mission. DOJ OIG intends to use statistical and mathematical techniques to identify high risk areas to conduct audits, and to identify activities that may indicate an investigation is warranted.

(b) The way the system operates to achieve the purpose(s):

> The DA Program operates to achieve this purpose by providing OIG: timely insights from the data already stored in DOJ databases that OIG has legal authorization to access and maintain;

---

[1] The IGNITE System Privacy Impact Assessment can be found at: https://www.justice.gov/OIG-IGNITE-PIA-11817/download.

[2] Unless otherwise indicated in this PIA Addendum, the DA Program incorporates the documented assessment conducted and published in the IGNITE System PIA.

the ability to monitor and analyze data for patterns and correlations that signal wasteful, fraudulent, or abusive activities impacting Department performance and operations; the ability to find, acquire, extract, manipulate, analyze, connect, and visualize data; the ability to manage vast amounts of data; the ability to identify significant information that can improve decision quality; and the ability to mitigate risk of waste, fraud, and abuse.

(c) The type of information collected, maintained, used, or disseminated by the system:

The information maintained within this system of records will be limited to information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs, operations, grantees, contractors, and associated personnel to recognize and mitigate fraud, waste, and abuse.

In connection with its broader oversight responsibilities relating to programs and operations of the Department to recognize and mitigate fraud, waste, and abuse, the DA Program will maintain and use data such as: DOJ accounting system information; DOJ grants management information; inmate processing, population management, and tracking information; inmate central records information; DOJ payroll information; DOJ data files required by the DATA Act (including but not limited to sampling of the spending data submitted in accordance with the DATA Act); DOJ charge card data (for example, travel, purchase, fleet and integrated card transactions); Federal contract actions whose estimated value is $3,000 or more, and every modification to such contract actions regardless of dollar value; Single Audit results (for example, results of a financial or compliance audit of recipients of Federal funds) and related Federal award information; Federal Bureau of Prisons (BOP) medical claim adjudication data; and Department employee worker's compensation payment data.

(d) Who has access to information in the system?

Only DOJ OIG employees and authorized contractors may have system user accounts. OIG Active Directories will be used for identification and authentication of users. Within the DA Program, access to data will be restricted with permissions set according to Memoranda of Understanding (MOUs) and the requirements of each user type. Specific access to sensitive PII data (including social security account numbers) is restricted further by user group and purpose, according to MOUs established and privacy policies.

(e) How information in the system is retrieved by the user:

For more information on how information is retrieved by system users, see the IGNITE System PIA.[3]

---

[3] *See supra* note 1.

(f) How information is transmitted to and from the system:

For more information on how information is transmitted to and from the system, see the IGNITE System PIA.[4]

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):

The DA Program will interconnect with other systems from various sources through established MOUs. Data sources include, but are not limited to:

- Internal (DOJ component) information systems, such as:
  - Grant Management System;
  - Federal Procurement Data System;
  - PaymentNet charge card transactions;
  - BOP Medical Expenses; and
  - DOJ financial systems.
- Other Federal agencies' datasets and systems, such as:
  - Department of the Treasury "Do Not Pay" information;
  - Department of Commerce Death Master Index;
  - Department of Labor worker's compensation information;
  - Department of Defense Contractor Performance Assessment Reports (CPARS); and
  - Department of Health and Human Services medical records information.
- Other data sources:
  - Publically available data; and
  - Purchased data sets (such as geo-coding data).

The information maintained within this system will be limited to information that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs, operations, grantees, contractors, and associated personnel to recognize and mitigate fraud, waste, and abuse.

(h) Whether it is a general support system, major application, or other type of system:

The DA Program is an application maintained within the IGNITE System boundary.

[4] *See supra* note 1.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

In connection with its investigative duties to recognize and mitigate fraud, waste, and abuse relating to Department programs, operations, grantees, contractors, and associated personnel OIG already maintains information on

- Individuals or entities who are or who have been the subject of investigations conducted by the OIG, including current and former employees of the DOJ; current and former consultants, contractors, and subcontractors with whom the Department and other federal agencies have contracted and their employees; grantees to whom the Department has awarded grants and their employees; and such other individuals or entities whose association with the Department relates to alleged violation(s) of the Department's rules of conduct, the Civil Service merit system, and/or criminal or civil law, which may affect the integrity or physical facilities of the Department.
- Individuals who are or have been witnesses, complainants, or informants in investigations conducted by the OIG.
- Individuals or entities who have been identified as potential subjects of or parties to an OIG investigation.
- Individuals currently or formerly under the custody of the Attorney General and/or BOP and/or United States Marshals Service (USMS).

In connection with its broader oversight responsibilities relating to programs and operations of the Department to recognize and mitigate fraud, waste, and abuse, OIG's DA Program will maintain the following information:

- Information maintained in DOJ system of records JUSTICE/DOJ-001, Accounting Systems for the Department of Justice, 69 Fed. Reg. 31,406 (June 3, 2004); 71 Fed. Reg. 142 (Jan. 3, 2006); 75 Fed. Reg. 13575 (Mar. 22, 2010); and 82 Fed. Reg. 24147 (May 25, 2017).
- Information maintained in DOJ system of records JUSTICE/OJP-004, Grants Management Information System, 53 Fed. Reg. 40526 (Oct. 17, 1988); 66 Fed. Reg. 8425 (Jan. 31, 2001); and 82 Fed. Reg. 24147 (May 25, 2017).
- Information maintained in DOJ system of records JUSTICE/USM-005, USMS Prisoner Processing and Population Management-Prisoner Tracking System (PPM-PTS), 72 Fed. Reg. 33515, 519 (June 18, 2007); 82 Fed. Reg. 24151, 163 (May 25, 2017).
- Information maintained in DOJ system of records JUSTICE/BOP-005, Inmate Central Records System, 67 Fed. Reg. 31371 (May 9, 2002); 77 Fed. Reg. 24982 (Apr. 26, 2012); 81 Fed. Reg. 22639 (Apr. 18, 2016); 82 Fed. Reg. 24147 (May 25, 2017).
- Information maintained in DOJ system of records JUSTICE/JMD-003, Department of Justice Payroll System, 69 Fed. Reg. 107 (Jan. 2, 2004); 72 Fed. Reg. 51663 (Sept. 10, 2007); 82 Fed. Reg. 24151, 158 (May 25, 2017).
- Department data files required by the DATA Act, including but not limited to sampling of the spending data submitted in accordance with the DATA Act.

- Department charge card data (for example, travel, purchase, fleet and integrated card transactions).
- Federal contract actions whose estimated value is $3,000 or more, that may be $3,000 or more, and every modification to such contract actions regardless of dollar value.
- Single Audit results (for example, results of a financial or compliance audit of recipients of Federal funds) and related Federal award information.
- BOP medical claim adjudication data.
- Department employee worker's compensation payment data.

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

In addition to the sources of information detailed in the IGNITE System PIA, the records within this system are sourced from public source materials; medical product and service providers; medical claim processing companies; financial institutions managing Department credit card and payroll information; and the system managers, or individuals acting on a system manager's behalf, for the DOJ and government-wide systems that OIG has legal authorization to collect and maintain as part of its responsibility to conduct, supervise, and coordinate audits and investigations of Department programs, operations, grantees, contractors, and associated personnel to recognize and mitigate fraud, waste, and abuse.

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.)

For more information on the identified and evaluated potential threats to privacy that exist in light of the information collected or the sources from which the information is collected, see the IGNITE System PIA.[5]

The aggregation of data from multiple sources for the DA Program results in some enhanced risks to privacy. The data above represents data that is or may be collected for OIG to analyze and help to effectively orient OIG efforts to areas where it can make the greatest difference in performing its mission to identify waste, fraud, abuse, and misconduct in Department operations, programs, grants, contracts, and by associated personnel. Such data aggregation may, for example, create a situation in

[5] *See supra* note 1.

which more information, from more sources, is collected than is necessary and relevant to help the OIG in its efforts to combat government fraud, waste, and abuse. In order to mitigate this risk, the DA program has established a Steering Committee, consisting of the Inspector General, high-level representatives from each of the OIG's divisions, and representatives from the OIG's Office of General Counsel. DA Program projects are undertaken in consultation with the IG and the Steering Committee, based on a defined objective and using methods that have been tested and validated. Additionally, the DA program mitigates the risk of faulty or incomplete data sources by conducting a multistep quality assurance process to validate data received from DOJ components.

In addition, the DA Program's focus on collecting and assessing large datasets to effectively orient OIG efforts results in some enhanced risks to privacy. In order to mitigate this risk, the DA program protects records using physical security methods and dissemination/access controls. Direct access is controlled and limited to approved personnel with an official need for access to perform their duties. Paper files are stored: (1) in a secure room with controlled access; (2) in locked file cabinets; and/or (3) in other appropriate GSA approved security containers. Protection of information technology systems is provided by physical, technical, and administrative safeguards. Information is located in a building with restricted access and are kept in a locked room with controlled access and/or are safeguarded with approved encryption technology. Multifactor authentication is required to access electronic systems. Information may be transmitted to routine users on a need-to-know basis in a secure manner and to others upon verification of their authorization to access the information and their need to know. Security personnel conduct periodic vulnerability scans using DOJ-approved software to ensure security compliance and security logs are enabled for all computers to assist in troubleshooting and forensic analysis during incident investigations. Users of individual computers can only gain access to the data by using a valid user identification authorization and authentication method. At no time are DA Program servers connected to the Internet.

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.)

In addition to the purposes outlined in the IGNITE System PIA, the DA Program will use this information to identify anomalies or indicators in the data that may evidence fraudulent or potentially criminal activity. The DA Program will also be used to improve audit quality by helping to identify specific areas of high risk for OIG attention or audit. The product of this work can be used by the OIG to identify areas to conduct audits or activities that may indicate that an investigation is warranted. The DA Program will also lessen the burden on DOJ components of providing data to the OIG for individual audits, inspections, reviews, and investigations, insofar as the OIG will already possess the data maintained by the DA Program.

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.

For more information on why the information that is collected, maintained, or disseminated is necessary to accomplish the above purposes and to further the OIG's mission, see the IGNITE System PIA.[6]

Many government oversight and law enforcement agencies are using data analytics to help identify and reduce fraud, waste, and abuse. Some data analysis methods are predictive, and can identify potential fraud or error before improper payments are made.[7] Other techniques, such as data matching, identify past activity and can help government agencies recover funds. These and other data analysis tools will assist the OIG in its mission of combating government waste, fraud, and abuse.

As noted above, even at this early stage, the DA program has been able to use BOP billing records to identify a health care provider who was billing as many as 61 psychiatric consultations in a single day. Even accounting for sessions coded as shorter consultations, this amounted to over 24 hours of service in a single day. As a result of this early work by the DA program, the OIG has issued specific recommendations to BOP to remedy its inadequate oversight of health care claims.

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.)

In addition to those authorities listed in the IGNITE System PIA, the DA Program is authorized under the following authorities:

	Authority	Citation/Reference
X	Statute	Inspector General Act of 1978, as amended, 5 U.S.C. App. § 3 (2012 & Supp. IV 2016); DATA Act, Pub. L. No. 113–101, 128 Stat. 1146. (codified as amended in scattered sections of 31 U.S.C.); Inspector General Empowerment Act of 2016, Pub. L. 114-317, 130 Stat. 1595 (2016).
	Executive Order	
	Federal Regulation	
X	Memorandum of Understanding/Agreement	Interface Agreement and Authorization to Use Data Between U.S. Department of Justice, Office

[6] *See supra* note 1.
[7] *See e.g.*, Government Accountability Office, GAO-13-680SP, Data Analytics for Oversight & Law Enforcement (July 2013) https://www.gao.gov/assets/660/655871.pdf (describing challenges, opportunities, and examples of successful uses of data-analytic systems to identify questionable claims for further investigations).

		of the Inspector General and U.S. Department of Justice, Office of Justice Programs, December 2016 Interface Agreement and Authorization to Use Data Between U.S. Department of Justice, Office of the Inspector General and U.S. Department of Justice, Justice Management Division, March 2017
	Other	

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. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records in the DA Program are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Job Number NI–60–97–4. For more information on 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, see the IGNITE System PIA.[8]

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.)

For more information on 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, see the IGNITE System PIA.[9]

The DA Program creates additional privacy risks insofar as inaccurate information can result in "false positives," potentially creating unintended consequences for individuals who are erroneously identified as the result of faulty data. However, the DA Program employs a multistep data quality management program to ensure that the data it has received is valid. In addition, the DA Program does not adjudicate any individual rights or entitlements. It identifies areas of risk so that audit and other resources can be more efficiently deployed, and it generates leads that must be substantiated by further investigation. As a result, individuals will never be denied a right, privilege, or benefit that the

[8] *See supra* note 1.
[9] *See supra* note 1.

individual would otherwise be entitled to by Federal law, or for which the individual would otherwise be eligible, based solely on a lead generated from the DA Program.

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.

For more information on whom OIG intends to share the information in the system and how the information will be shared, see the IGNITE PIA.[10]

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: Information utilized by the DA Program will be sources from other systems, not directly from individuals to whom the PII may pertain.

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:

[10] *See supra* note 1.

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Information utilized by the DA Program will be sources from other systems, not directly from individuals to whom the PII may pertain.

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.

Information utilized by the DA Program will be sources from other systems, not directly from individuals to whom the PII may pertain. To the extent that information contained in the DA Program is protected by Federal law, including the Privacy Act, notice is provided by a DOJ Privacy Act System of Records Notice (SORN), detailed in Section 7. These notices and documents are published in the Federal Register and on the Department's SORN webpage,[11] and are available to the general public. For more information on the notices related to this, see the IGNITE System PIA.[12]

Section 6: Information Security

For more information on how information will be secured, including how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access, see the IGNITE System PIA.[13]

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created or has already been created in accordance with 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:

[11] The DOJ Privacy Act SORN webpage can be found at: https://www.justice.gov/opcl/doj-systems-records.
[12] *See supra* note 1.
[13] *See supra* note 1.

	• JUSTICE/OIG-006, Data Analytics Program Records System, 83 Fed. Reg. 13309 (Mar. 28, 2018).
☐	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.

Records in this system of records can be retrieved by name or other identifiers, including, but not limited to: the surnames of subjects, witnesses, and/or complainants of an OIG complaint or investigation; social security account number; address; telephone number; OIG-assigned case numbers; taxpayer identification number; health care provider; assigned number given to an individual in custody with USMS; inmate register number; alien registration number; assigned DOJ charge card information; geo-code location (for example, physical addresses converted into geographic coordinates on a map); organizational name; employee payroll identifier; and Data Universal Numbering System (DUNS number).