OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

CONGRESSIONALLY DIRECTED REPORT FOR THE OFFICE OF INSPECTOR GENERAL'S DATA ANALYTICS PROGRAM

DOE-OIG-24-36

APRIL 2024

Department of Energy
Office of Inspector General
Washington, DC 20585

April 17, 2024

The Honorable Patty Murray
Chair
Senate Committee on Appropriations
154 Russell Senate Office Building
Washington, D.C. 20510

The Honorable John Kennedy
Ranking Member
Subcommittee on Energy and Water Development
Senate Committee on Appropriations
437 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Chuck Fleischmann
Chair
Subcommittee on Energy, Water Development, and Related Agencies
House Committee on Appropriations
2187 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Marcy Kaptur
Ranking Member
Subcommittee on Energy, Water Development, and Related Agencies
House Committee on Appropriations
1036 Longworth House Office Building
Washington, D.C. 20515

Dear Chairwoman Murray, Chairman Fleischmann, Senator Kennedy, and Congresswoman Kaptur:

The Joint Explanatory Statement that accompanies the Energy and Water Development and Related Agencies Appropriations Act, 2024, includes a requirement for a report to the Committees regarding the Office of Inspector General's collection of payroll-related information from the Department of Energy's contractors. I am pleased to present you with the requested information in the attachment to this letter.

I would be happy to meet with you to discuss this information and to answer any questions you may have.

Sincerely,

Teri L. Donaldson
Inspector General

Attachment

Attachment

Congressionally Directed Report for the Office of Inspector General's Data Analytics Program
Fiscal Year 2024 Appropriation
Department of Energy

The joint explanatory statement from the Energy and Water Development and Related Agencies Appropriations Act, 2024, includes a requirement for the Department of Energy's Office of Inspector General (OIG) to issue a report to the Committees on Appropriations of both Houses of Congress regarding the OIG's collection of payroll-related information from Department contractors. In response, the OIG is providing this report detailing our data analytics efforts—efforts that are well within the recognized authority of the OIG, are being conducted securely in accordance with the Privacy Act of 1974 (Privacy Act), and form a key part of the OIG's strategy to prevent, detect and deter fraud, waste, and abuse by Department contractor personnel.

I. Executive Summary

The purpose of the data request referenced in the joint statement is, as a part of a suite of activities, to assess, detect, and deter payroll-related fraud[1] within the Department's complex. To do so, the OIG is using data analytics to support risk assessments and subsequent audits, evaluations, inspections, investigations, and reports. Approximately 90 percent of the Department's base funding goes to its prime contractors. Many of those contractors are performing highly sensitive work in Government-owned facilities. Therefore, our efforts to prevent fraud, waste, and abuse at the Department must include oversight of the contractors.

The OIG's initial request for payroll-related data was made to a single contractor in September 2021. In response to that request, the contractor provided the requested data within 45 days. In March 2022, the OIG expanded the inquiry to 10 additional prime contractors at 5 sites. Only recently, in March 2024, have the last contractors complied with this request, which is unacceptable. Primarily using data provided by the earlier cooperating contractor, the OIG uncovered fraudulent activities resulting in more than 20 active criminal investigations, indictments, and convictions specific to pandemic-era fraud.

The information requested by the OIG is data routinely collected and maintained by the human resources element of each contractor.[2] When the OIG requested the data, the contractors raised various concerns. However, there was no legal or practical reason for delaying delivery of this data to the OIG for 2 years. As discussed in this report, the data transferred to the OIG remains fully secured and is subject to all applicable legal requirements and security protections. While addressing the concerns from the contractors, the OIG discovered that the Department does not maintain a current list of the identifiers that would allow the Department to identify the contractor employees working at these sensitive sites without first making inquiries to each contractor.

---

[1] *FY 2023 Department of Energy Agency Financial Report* (page 12, November 2023). The Department reports a total of 16,417 Federal employees and 124,460 contract employees.

[2] The requested data from the 10 contractors across 5 sites included: employee employer; employee title; employee name; employee unique identifier; service computation date; separation date; salary; last four digits of social security number; home address (city, state, zip code); phone number; and email.

Data Analytics Is Foundational to Modern Management, Policymaking, and Oversight

The use of data analytics allows an organization to evaluate transactional data in support of decision making regarding policy, program operations, resource allocations, risk management, and mission outcomes. Effective enterprise data analytics and its supporting foundational infrastructure enable modern and more effective management approaches. Federal laws and provisions have been established over the years to ensure that the management and use of data is prioritized within Federal agencies. Supplemental guidance and leading practices from a variety of recognized sources build on existing legal provisions and requirements, all of which assist agencies with incorporating data analytics to combat fraud and ensure integrity, efficiency, and integration of programs and operations.

Despite increased Federal efforts to promote information as a valuable national resource and strategic asset, the Department is lagging behind comparable peers. The Department lacks the data and governance structure necessary to make critical decisions or gain visibility into program objectives.[3] The Department's distributed and decentralized environment further exacerbates already existing data access and management challenges. Such an environment hinders the Department's ability to provide effective oversight and detect fraud, enhance data-driven management, realize performance improvement, and reduce risk to Federal resources, including security-related risks.

For 34 years,[4] the Department has been a mainstay on the Government Accountability Office's (GAO) High-Risk List for its acquisition and management of contractor resources. The Department's decision making will continue to be ill-informed without effective data management and analytics processes in place to help guide decisions using real and authoritative data, including data from its major contractors. Going forward, if the Department does not make progress improving its data collection, sharing, and analytics protocols, it is unlikely that it will be able to move away from a "pay and chase" model and toward prevention, early detection, and response to fraud, waste, and abuse.[5] Without improvements, we do not see a path for the Department to sufficiently enhance its operations to warrant removal from the GAO's High Risk List.

The Full Scope of Pandemic Fraud May Never Be Known but Already Is Shocking

The OIG's use of data analytics to evaluate payroll data is a key component to ensuring that COVID-19 relief funds targeting income security[6] were properly used by the Department's contractor employees. In an analysis, the Associated Press "found that fraudsters potentially stole more than $280 billion in COVID-19 relief funding; another $123 billion was wasted or misspent. Combined, the loss represents 10 percent of the $4.2 trillion the U.S. [G]overnment has […] disbursed in COVID relief aid."[7] The Small Business Administration's OIG found that up to $200 billion may have been stolen from just two programs—the Paycheck Protection Program (PPP) and the Economic Injury Disaster Loan Program (EIDL).[8] As quoted in its report, "This means at least 17 percent of all COVID-19 EIDL and PPP funds were

[3] *The Department of Energy's Considerations and Use of Data Analytics* (DOE-OIG-24-14, March 2024) discusses the legal frameworks, leading practices, benchmarking, past oversight, initial progress, and impact for the Department's use of data analytics. The Department agreed with enumerated considerations.
[4] Original GAO High Risk Letter (January 23, 1990).
[5] *The Department of Energy's Considerations and Use of Data Analytics* (DOE-OIG-24-14, March 2024) discusses the "pay and chase" model.
[6] The OIG focused on use of the EIDL and the PPP.
[7] The Great Grift: How billions in COVID-19 relief aid was stolen or wasted | AP News.
[8] COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape | U.S. Small Business Administration (sba.gov).

disbursed to potentially fraudulent actors." Despite the Department contractors' resistance to OIG oversight, the OIG has already successfully used data analytics to discover that the Department's complex was not immune to this looting of the Federal Treasury.

Crystalizing the key prescription, Michael Horowitz, Chair of the Pandemic Response Accountability Committee (PRAC), has highlighted the central role of access to authoritative data and the use of data analytics as foundational tools in the success of the PRAC's Pandemic Analytics Center of Excellence (and other Inspectors General) to detect fraud and improve Federal program integrity and operations. His points were reinforced by previous lessons learned from experiences with the Recovery Accountability and Transparency Board after the 2008–2009 financial crisis and recovery.[9]

The OIG Is Securely and Appropriately Integrating Data Analytics, While Engaging With Stakeholders

The OIG is using data analytics across our mission, as described in our *Semiannual Reports to Congress*.[10] The OIG data analytics program ensures data safeguards through a comprehensive suite of management, technical, and operational measures that collectively address the confidentiality, integrity, and availability of data. We also have fully integrated treatment of the Fair Information Practice Principles as reflected in the Privacy Act. The OIG recognizes the benefit of promulgating a data analytics "system of records notice" (SORN) to further support the mission of our Office of Cyber Assessments and Data Analytics. While the OIG could continue conducting data analytics activities under its current SORNs,[11] the new SORN increases our engagement with stakeholders and further strengthens our efforts to establish a shared understanding of the OIG's mission and authorities across the Department's complex.

OIG Funding Related to the Data Request

Funding for the data request at issue here was sourced from the OIG's base appropriation. The OIG leveraged its existing information technology infrastructure to support the data collection effort referenced here, resulting in no additional costs for storage of the data. The cost associated with the collection, security, and maintenance of the contractor data is negligible because the specific data referenced in the joint statement is relatively small. The data was not a factor in the OIG's sizing and securing of its data analytics technical infrastructure.

With respect to the cost of analyzing the data, we estimate those costs will range from $225,000 to $275,000 in fiscal year (FY) 2024. We anticipate the results of this work will return monies to the Government well beyond that cost.

The OIG did not separately track the unnecessary and wasteful cost of resolving the resistance to oversight for the OIG, the Department, or for the contractors that may be requesting reimbursement for those costs.

---

[9] Statement of Michael E. Horowitz Chair, PRAC Inspector General, U.S. Department of Justice before the U.S. Senate Committee on Homeland Security & Governmental Affairs Emerging Threats and Spending Oversight Subcommittee concerning "Examining Federal COVID-era Spending and Preventing Future Fraud."

[10] Semiannual Reports to Congress | Department of Energy.

[11] The OIG has two existing SORNs, DOE-54 and DOE-83, that address investigations and allegation-based inspections, respectively. The SORNs facilitate the discovery of fraudulent activity, including with respect to all investigative stages of investigations whether civil, criminal, or administrative.

II. Discussion

1. Purposes for the Information Collected and the OIG's Data Analytics Program

The purpose for the OIG's information collection was to assess risks for a variety of payment-related issues and identify potential fraud. Our initial efforts have enhanced Federal program integrity efforts, despite receiving limited cooperation in collecting requested data.[12] Under the authority of the Inspector General Act of 1978, the OIG conducts data analytics to assess risk as well as to detect and deter fraud, waste, and abuse in Department programs and operations. The OIG also uses data analytics to provide the Department with recommendations to address identified risks and challenges. Our integration of data analytics is central to streamlining our processes while increasing the strategic impact of our independent oversight. The anomalies we detect serve as a valuable first step in determining where to allocate scarce resources to determine whether targeted risks are systemic to the Department or specific to a program or site, and if violations have occurred. Our existing authorities cover the program as implemented. Existing authorities allow—indeed encourage—the use of data analytics consistent with our current use.[13]

Early Results Establish the Risk of Pandemic-Related Payroll Fraud to the Department

Using the information gathered early in these efforts, the OIG has identified criminal activity by multiple contractor employees. Work continues on recently received data from the 10 major contractors across the 5 sites that resisted oversight.

Without our collection and analysis of specific data, it is unlikely that those committing the fraud would have been identified. The resistance of the Department's contractors to OIG oversight in this area has made it difficult to detect fraud, diminished the timeliness and effectiveness of our results, reduced the Department's deterrence to fraud, and wasted scarce resources.

A majority of the criminal matters we are currently investigating under this data analytics effort involve false statements and claims made to the Government by bad actors within its trusted workforce. The Government takes great care in vetting people who work in sensitive areas. It is vitally important for the Department to be able to timely identify potential wrongdoing by individuals working in the agency's highly sensitive facilities, whether those individuals are employed by the Department or located at one of the Department's Government-owned, contractor-operated facilities.

In addition to protecting the existing mission elements of the Department from the risks of employing criminals, identifying and prosecuting these individuals with alacrity is an obvious first step toward deterring fraud and protecting the Department's new mission elements being funded at unprecedented levels. These new mission elements have been funded under the Infrastructure Investment and Jobs Act (IIJA), Inflation Reduction Act (IRA), and Puerto Rico Energy Resilience Fund (PR-ERF). Our data analytics

[12] The OIG's last *Semiannual Report to Congress* (DOE-IG-0084), pages 14–16, reported continued substantial delays in receiving the information referenced in the agreement language requested from 10 major contractors at 5 Department sites—information that the OIG is authorized to access pursuant to the Inspector General Act of 1978. The OIG received the data from the last contractor at the last site on March 20, 2024.

[13] *The Department of Energy's Considerations and Use of Data Analytics* (DOE-OIG-24-14) discusses legal and policy encouragement and mandates for the use of data analytics, in particular for payment integrity efforts, and to prevent, detect, and deter fraud, waste, and abuse.

program has given us actionable insights to extend that prophylactic work, complementing the OIG's Hotline as one source that leads to investigations and other OIG work, and providing a tool for understanding the Department's risks.

The OIG Is Using Data Analytics to Modernize and Scale the Impact of Its Independent Oversight

Current focus areas for the OIG's use of data analytics include but are not limited to: payroll fraud; procurement collusion; grant fraud and research security; public corruption; and fraud, waste, and abuse. These programs and operations are funded with base, IIJA, IRA, and PR-ERF appropriations. Specific requests for data by the OIG from across the Department's complex are risk-prioritized, with the requested data elements determined as needed to meet the determined and authorized scope. We pursue these prioritized targets as we can within available appropriations.

These focus areas for data analytics risk assessments and support for specific matters are based on law and policy, past oversight, established leading practices, and our understanding of the Department's risks, challenges, and management and operating culture. GAO and OIG reports and investigations have established challenges and (high) risks across the complex.[14] Daniel Glad, Director of the Department of Justice's Procurement Collusion Strike Force, recently identified that "governments around the world pay 20 percent more because of bid rigging, price fixing, and other collusive schemes."[15] The Association of Certified Fraud Examiners states that "the typical organization loses about 5 percent of its revenues to fraud."[16] The GAO has identified insufficient competition in the Department's procurements[17] and the extensive use of subcontractors with opaque beneficial ownership[18] as drivers of inflated costs.

The OIG Office of Investigations currently has approximately 300 open matters (i.e., complaints and active investigations) that span a wide range of Department facilities, programs, and activities, aligned against and in part driving the priorities previously described. For example, predicated Hotline complaints related to timecard and payroll irregularities (i.e., fraud) with the Department's contractors are fast growing,[19] and comprised about 15 percent of our total predicated complaints in FY 2023. The Department's risk profile, and our analysis of reported levels of improper payments,[20] suggests that the Department's lagging adoption of data analytics powered by authoritative data across its complex is heightening the risk of undetected, undeterred, and unprevented fraud, waste, and abuse across the complex.

---

[14] For example, the OIG's Special Report, *Management Challenges at the Department of Energy — Fiscal Year 2024* (DOE-OIG-24-05, November 2023).

[15] "Remarks to the National Association of State Procurement Officials' 10th Annual Law Institute," November 23, 2023.

[16] "Organizations Worldwide Lose Trillions of Dollars to Occupational Fraud" (March 30, 2022).

[17] "Department of Energy Contracting: Additional Actions Could Further Strengthen Competition" (January 24, 2023).

[18] "Department of Energy Contracting: Actions Needed to Strengthen Subcontract Oversight" (March 12, 2019).

[19] In FY 2022, the corresponding number was about 10 percent; in FY 2021, about 5 percent. Note that separately the OIG has been working with the Department in the corresponding period to improve mandatory disclosure and reporting from its contractors with some success. We see this growth in reporting as likely reflective due to those efforts.

[20] For example, the OIG's Report, *The Department of Energy's Payment Integrity Reporting in the Fiscal Year 2022 Agency Financial Report* (DOE-OIG-23-22, May 2023).

OIG's Leadership Should Accelerate the Department's Adoption and Use of Data Analytics

Because the Department and the OIG have broad legal access to these Government-owned, contractor-operated facilities and records, and because data analytics is a proven leading practice, the Department's use of data analytics should be increasing at a substantial rate. It is not. The OIG is integrating the use of data analytics across its operations. However, the OIG's use of data analytics is no substitute for the Department's obligation to adopt leading practices to improve its management and oversight of its programs and operations. The Department has a long way to go to implement data analytics and to use its own data as a strategic enterprise asset.[21] In the meantime, the OIG's organic data analytics capability is reducing risk and cost to the Department.

2. Estimated Cost and Sources of Funds for Data Collection and Storage Prior to the Enactment of This Act

Funding for this data request was sourced from the OIG's base appropriation. The OIG leveraged its existing information technology infrastructure to support the data collection effort referenced here, resulting in no additional costs for storage of the data. The cost associated with the collection, security, and maintenance of the contractor data is negligible because the specific data referenced in the joint statement is relatively small. These costs were not a factor in the OIG's sizing and securing of its data analytics technical infrastructure.

The OIG did not separately track the cost of resolving the inappropriate resistance to oversight for the OIG, the Department, or for the contractors that may be requesting reimbursement for those costs.

3. Estimate of Costs Associated with Collecting, Analyzing, Securing, and Maintaining the Data

The OIG expects no additional costs for collecting, securing, and maintaining the data going forward, for the same reasons already discussed. With respect to the cost of analyzing the data, we estimate those costs will range from $225,000 to $275,000 in FY 2024. We anticipate the results of this work will return monies to the Government well beyond that cost.

In FY 2024, the OIG estimates that it will spend approximately $6.8 million on its data analytics program. This includes $3.5 million for 14 Federal full-time employees and $3.3 million in contractor and technology costs to support information technology infrastructure development and operations, including safeguarding, maintenance, data analysis, and visualization. Where we are supporting an oversight matter, we allocate the cost to the corresponding account(s). Future OIG costs for data analytics are variable based on availability of appropriations, scope, and focus for upcoming risk-prioritized assessments and risk-prioritized specific matters. We have flexibility as to deploying new capability, how many risk assessments we conduct, and how many matters we support.

[21] The OIG published a Special Project Report, *The Department's Considerations and Use of Data Analytics* (DOE-OIG-24-14, March 2024). The OIG would prefer to conduct risk prioritized auditing of the integrity of the Department's data feeds and risk modeling, but the Department has yet to develop these capabilities.

The OIG's Strategic Plan[22] includes discussion of purpose and use of funds to advance use of data analytics. Our FY 2023 performance report[23] discusses the OIG's substantial results within our available appropriation, supported in part through our data analytics program. To date in FY 2024, the Data Analytics Division has supported 38 proactive and objective risk-based projects and more than 16 other discrete requests. The OIG continues to use data analytics to assess risks and advance specific audits, inspections, evaluations, investigations, and other matters spanning the Department's base, as well as IIJA-, IRA-, and PR-ERF-related activities.

The OIG has briefed Congress on the OIG's resource gaps within our base and IIJA and IRA appropriations. The OIG has also highlighted these gaps in the President's Budget, testimony before Congress, and in our reporting. The OIG appreciates that Congress increased our IIJA and IRA oversight accounts in the FY 2024 Enacted Budget. We are integrating that increase into our planning and are looking forward to working with Congress to close remaining resource gaps, including in our base appropriation. Subject to availability, the OIG plans to use funding from our base, IIJA, IRA, and PR-ERF appropriations to scale and accelerate our data analytics activities and close noted oversight shortfalls.

4. Safeguards Used by the Department and the OIG

The OIG data analytics program ensures data safeguards through a comprehensive suite of management, technical, and operational measures that collectively address the confidentiality, integrity, and availability of data. In addition to adhering to the National Institute of Standards and Technology's Risk Management Framework Moderate Security Baseline, the OIG's data analytics program operates in a secure architecture which exceeds the moderate requirements for certain controls. Due to the nature of the data, aggregation of data, our independent mission, and our assessment of risk, the OIG implements additional required controls towards a High Security Baseline.

The OIG provisions its data analytics information technology infrastructure fully within the security boundaries of the Department's Enterprise Information Technology Systems shared services environment. We integrate encryption of data in transit and at rest, role-based access controls, multi-factor authentication, and a comprehensive monitoring program alongside measures for physical security. To further enhance data protection, the OIG incorporates advanced data management practices such as data segmentation and anonymization or masking, which prevent the compilation of data from revealing sensitive information not apparent in the individual data sets. The OIG also employs data management practices such as row- and column-level security and data sensitivity to reinforce the integrity of our operations and support assurance of authorized use of data.

5. Applicable Policies That Exist to Protect Sensitive Data From Abuse or Disclosure, Including Limits on Accessing the Data Only for Official Purposes

The OIG data analytics program operates under the Department's cybersecurity, privacy, and records retention policies and operational processes. The data analytics SORN will comply with those policies and processes as well as the Privacy Act.

The SORN, while claiming certain exemptions under the Privacy Act, does so in a manner consistent with the practices of Federal law enforcement agencies. Exemptions from Privacy Act provisions such as 5

[22] *U.S. Department of Energy Office of Inspector General, Strategic Plan, Fiscal Years 2022 – 2026*.
[23] *Fiscal Year (FY) 2023 Annual Performance Results*.

U.S.C. § 552a(e)(1) (referring to maintaining only relevant and necessary information) and (e)(5) (referring to maintaining accurate, relevant, timely, and complete records) are necessary to protect the integrity of the OIG's data analytics efforts.

As explained in the Notice of Proposed Rulemaking (NOPR) issued on November 27, 2023, the exemption from 5 U.S.C. § 552a(e)(1) is necessary because in the course of investigations into potential violations of Federal law, and in the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity even if the information obtained may not be initially viewed as strictly relevant or necessary. For example, in a data analytics effort to evaluate procurement collusion, it may not be immediately obvious what transactions are suspect until after the data matching occurs. Similarly, as explained in the NOPR, the exemption from 5 U.S.C. § 552a(e)(5) is necessary because the OIG is sometimes unable to vouch for the accuracy and completeness of the information maintained by others. For example, in the OIG's recent effort to evaluate payroll data to ensure COVID-19 relief funds were properly used, the contractor payroll data was retrieved from various contractors. The information received by the OIG is only as good as the information maintained by the contractors. Consequently, the Privacy Act exemption recognizes that the OIG may have reason to obtain the information but may not be able to attest to the accuracy without further efforts.

The OIG remains committed to upholding the principles of the Privacy Act, applying exemptions judiciously, and to balancing its investigative responsibilities with the protection of individual privacy rights. Additionally, as described in the following table, the OIG data analytics program has considered the Fair Information Practice Principles, as reflected in the Privacy Act, in its design and operations of its policy, processes, and technical infrastructure.

Fair Information Practice Principle	OIG Commitment
Access and Amendment. Agencies should provide individuals with appropriate access to personally identifiable information (PII) and appropriate opportunity to correct or amend PII.	The OIG has the legal authority to maintain such records without individual participation through widely adopted exemptions to the Privacy Act used across the law enforcement and national security communities.
Accountability. Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors and should provide appropriate training to all employees and contractors who have access to PII.	The OIG data analytics program follows Department guidelines regarding safeguarding PII in Section 4(b)(1) of Department Order 206.1A, *Department of Energy Privacy Program*. Specifically, the OIG ensures compliance with privacy requirements; protects PII from unauthorized access or disclosure; limits the collection to only that information specifically needed for data analytics and the OIG mission; minimizes the use of social security numbers when possible; and ensures annual training on identifying, safeguarding, handling, and protection of PII. In compliance with Section 4(b)(2)(b) and 4(b)(3), the OIG also provides a SORN and complies with the applicable Privacy Compliance Requirements, respectively. We operate under the Department's cybersecurity and privacy policies and operational management.

Fair Information Practice Principle	OIG Commitment
	We collectively publish principles and standards that govern our work via the Council of the Inspectors General on Integrity and Efficiency. These principles and standards emphasize fairness, quality, and objectivity. Inspectors General are subject to oversight via peer reviews, by Congress, and through Congressionally directed oversight from the GAO.
Authority. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.	The OIG data analytics program derives its authorities from the Inspector General Act of 1978, the Inspector General Empowerment Act of 2016, and Department Order 221.2A.
Minimization. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.	The OIG data analytics program collects, uses, processes, stores, and maintains data to support audits, evaluations, inspections, or investigations. The use of this data will vary based on OIG requirements. PII is collected for purposes directly related to the organizational needs and are masked unless unmasking is required for a specific purpose. PII is disseminated or disclosed as required for the furtherance of specific risk assessments, audits, evaluations, inspections, or investigations.
Quality and Integrity. Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.	The OIG data analytics program collects PII from original sources, and, to the extent practical, ensures that the PII is accurate, relevant, timely, and complete. Because of the standards in which it operates and amplified by the need for rigor in its risk modeling, the OIG has a strong focus on lineage and provenance of its acquired data and key aspects of quality and integrity. Any data analytics results are carefully reviewed and vetted to minimize false positives.

Fair Information Practice Principle	OIG Commitment
Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.	The Privacy Act allows Government agencies to exempt certain records from the access and amendment provisions. The OIG has in place standard law enforcement and national security exemptions as the OIG has the legal authority to maintain such records without individual participation.
Purpose Specification and Use Limitation. Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.	The Department's privacy banner advises users that data collection may be used for multiple Government purposes. The OIG data analytics program aggregates, stores, and uses data that the OIG has the legal authority to collect and maintain to perform statistical analytics, data science, link analysis, and other mathematical techniques. The goal of this work is to identify anomalies that may indicate systemic or specific risks as well as activities that indicate mismanagement, fraud, abuse, waste, and unlawful or unethical activity in Department programs and operations.
Security. Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.	Note: Security safeguards are detailed above in the section titled "Safeguards Used by the Department and OIG."
Transparency. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.	The Department's privacy banner advises users that data collection may be used for multiple Government purposes. Due to OIG involvement in administrative, civil, and criminal investigations, suitability matters, and classified matters, the OIG has several exemptions in accordance with the Privacy Act. The OIG's proposed new SORN increases our engagement with our stakeholders and will continue our efforts to establish a shared understanding of the OIG's mission and authorities across the Department's complex.

6. Estimated Length of Time the Collected Data Will Be Retained

The OIG follows Federal and Department data retention policies. The data is stored according to the appropriate records schedule. If the data matching result is used in an audit, inspection, or investigation, the data matching result will follow the retention schedule for that action. For such matters that do not develop into the initiation of a more formal OIG action, there is a 10-year retention period for information or allegations which are of an investigative nature but do not relate to a specific allegation.[24] The OIG is evaluating its records retention requirements in order to ensure adherence to best policies and practices, which will include re-evaluating the appropriate retention periods for data analytics records. Such an evaluation would consider OIG mission needs as well as the Fair Information Practice Principles.

7. Aggregation of Data

As previously described, the OIG has already applied several safeguards based on its assessment of risk, including considering the risk of data aggregation. With each new data request, the OIG evaluates updating its assessment of risk based on the specific requested data and proposed aggregation of that data.

[24] Department Administrative Records Schedule 22, Audit/Investigative Records (Revision 4), N1-434-00-1, Item 4 (October 2021). The cut-off for the records is the end of the FY.