Privacy Impact Assessment
for the

Dashboard Management Reporting System (DMRS)

March 16, 2018

Contact Points

Ruth Shearer
System Owner
OCIO/NBIB IT PMO

Bruce Hunt
Acting Product Owner
NBIB/ITMO/PO

Reviewing Official

Kellie Cosgrove Riley
Chief Privacy Officer

Abstract

The United States Office of Personnel Management (OPM) National Background Investigations Bureau (NBIB) conducts background investigations, reinvestigations, and continuous evaluations of individuals under consideration for, or retention of, Government employment. The purpose of the Dashboard Management Reporting System (DMRS) is to provide statistical reports to authorized users to support the management and reporting of the investigative process timeliness and workload. This Privacy Impact Assessment (PIA) is being conducted because the DMRS processes Personally Identifiable Information (PII) about applicants who are undergoing a background investigation and others whose information may be included in background investigation files or in other systems maintained by OPM.

Investigation Overview

The NBIB conducts background investigations for Federal government agencies to use as the basis for suitability and security clearance determinations as required by Executive Orders and other rules and regulations. The NBIB is responsible for most of the Federal government's background investigations, conducting millions of investigations each year on Federal applicants and employees, active military personnel, government contractors, and private sector employees in positions regulated by the government. In addition, the NBIB has other responsibilities, including processing and providing informational reports within the NBIB and to external agencies.

The background investigations consist of several major activities which involve multiple the NBIB IT systems. The investigation process is initiated when a sponsoring agency requests an investigation of an identified candidate. The candidate then completes and submits various investigative forms. The information the candidate submits is reviewed and screened by the sponsoring agency's personnel security officer (or designee), who then submits the request for processing thru the NBIB's Electronic Questionnaire for Investigations Processing (e-QIP), a system that provides a means to facilitate the processing of standard investigative forms.

Interviews with the candidate and other people related to the investigation are then scheduled and assigned to an investigator or investigators by the Personnel Investigation Processing System (PIPS). The PIPS is the primary system for the processing, storing and administration of background investigations on candidates for national security, public trust and non-sensitive positions within the Federal Government. In addition other relevant information is gathered (e.g., employment, credit, criminal history), and the investigators then produce various Reports of Investigation (ROI). The ROI is then reviewed for completeness and a general case review is conducted. The case is then closed and prepared for delivery. An electronic or printed paper file is then sent to the sponsoring agency, which makes the final decision/adjudication regarding the candidate's investigation. When the sponsoring agency makes its decision regarding the candidate's investigation, it returns the decision/adjudication to the PIPS system for record keeping.

System Overview

The DMRS, built using a commercial off the shelf business intelligence software product, is used to create statistical and summary reports for the investigative process based on information in the DMRS database. It offers a fully integrated set of capabilities that allows users to perform queries with sorting, filtering, and drill down capability through a web browser. The DMRS database, or data warehouse, is data extracted (once per day) from the Personnel Investigative Processing System (PIPS) with approximately 95% of the PIPS data copied into the DMRS data warehouse. The information from PIPS contains master data on the subject of the investigation, to include identifying information such as the subject's name, date of birth, and Social Security number, as well as process information, such as what information needs to be collected about the subject (e.g., employment, education).

Using DMRS, authorized NBIB users can run various types of reports: business intelligence reports, which include statistical reports that illustrate trends over time and workload reports specific to various NBIB organizations; daily statistical reports, which provide agencies with information concerning their submissions to NBIB from the previous day to

assist those agencies in determining whether their submissions were received and whether there were any issues with their submissions; and ad hoc reports, which an authorized user might run to obtain information on a discrete, non-recurring question that arises in the course of NBIB operations.

These reports can be run on an ad hoc basis, in which users can build a query and obtain results in PDF, HTM or Excel spreadsheet format. Reports can also be done on a repetitive basis. Users can also create a report query and place it in a domain, or functional area, of the system. These domains are aligned to the various business functions within NBIB. All authorized users of that particular domain can then access the report and run it as needed. Finally, there are reports that are automatically scheduled in the system to run on a recurring basis (e.g., daily, weekly, monthly), that do not require human intervention in order to run and send to pre-populated email addresses.

The DMRS also utilizes a geospatial mapping system to produce interactive maps identifying the geographical breakdown of investigative information. This permits the user to illustrate, for example, the work that needs to be done in a particular location, such as employment or education checks, and the number of investigators that are assigned there. The mapping capability allows geographical representation of metrics for such things as work that is pending or past due. In addition, drill down capability exists so that a user can, for example, click a hot spot on a map to produce a detailed report and move from reports to maps.

In addition to the reports that are generated from the PIPS data in the DMRS database, DMRS also has read-only access to other systems and runs reports based on the information in those systems. DMRS does not store any information from those sources. Relevant to the NBIB investigation process, DMRS queries selected FTS data in real-time, utilizing database views, to create statistical and workload reports. These support the overall management of FTS, which processes all fingerprint transactions between OPM and the FBI, and enhances NBIB's reporting to their customers. Unrelated to the NBIB investigation process, the OPM Office of the Chief Information Officer uses DMRS to generate reports based on information in the Serena Business Manager (SBM), a process management and change

control system that is used to organize and manage software development projects.

DMRS is also used to generate reports based on information in the Executive and Schedule C System (ESCS). ESCS is administered by OPM personnel in OPM's Employee Services (ES) office. The system contains information about current and former appointees in the Senior Executive Service and other senior level employees, including Schedule C appointees. The reports run using DMRS include reports that illustrate the number of positions allocated to an agency and the number filled, reports on the names and other information of individuals who have completed SES candidate development training, and other reports that provide both statistical and individual-level information about senior executives. OPM ES users of DMRS can write a query in DMRS, which then connects to ESCS where it has read-only access to only those files necessary to run the particular report. DMRS runs the query and returns the relevant report in html, Excel, PowerPoint, or pdf format. Authorized users of ESCS from other agencies can also request reports but do not have direct access to DMRS. Instead, they can make a request for a report on a reports page in ESCS that, if approved, causes the report to be run and displayed in ESCS.

Section 1. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

5 C.F.R. parts 2, 5, 731, 732, 736, and 1400 establish the requirements for agencies to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. Depending upon the purpose of the particular background investigation, OPM is authorized to collect information under Executive Orders 9397, 10450, 10577, 10865, 12333, 12968, 13467 as amended, 13488, and 13549; 5 U.S.C. §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b) (3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; and Homeland Security Presidential Directive (HSPD) 12.

5 C.F.R. §§ 9.2 and 214.203 support the collection of the information in ESCS for reporting purposes.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The SORN that applies to the records contained in DMRS, as well as to the records in FTS on which FTS runs reports, is OPM/CENTRAL 9 Personnel Investigations Records which can be found at www.opm.gov/privacy. The SORN that applies to the records in ESCS that are used to generate reports in DMRS is OPM/Central 13, Executive Personnel Records.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes, the DMRS System Security Plan (SSP), Version 3.0, February 22, 2017 was completed as part of the system's Authorization to Operate (ATO) on March 21, 2017.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes, records schedule N1-478-08-002 applies to the investigation records in DMRS. Records schedule N1-478-95-003 applies to the records in ESCS that are used by DMRS to generate reports.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information that is contained in ESCS and used by DMRS is not subject to the PRA. The DMRS uses some of the information that individuals record on the forms listed below for the NBIB reports, such as the questionnaire for non-sensitive positions, national security positions, and fingerprint chart

respectively. The Office of Management and Budget (OMB) control numbers for the initial collections are:

Form Number	Form Name	OMB Number
SF-85	Questionnaire for Non-Sensitive Positions	3206-0261
SF-85P	Questionnaire for Public Trust Positions	3206-0258
SF-86	Questionnaire for National Security Positions	3206-0005
SF-87	Fingerprint Chart	3206-0150
SF-85P	Questionnaire for Public Trust Positions	3206-0191

Section 2. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The DMRS copies the following information from PIPS: first name, last name, address, phone number, aliases used, Social Security Number (SSN), Date of Birth (DOB), Place of Birth (POB), educational information, financial information, personal conduct, legal information, medical information, employment information, and other information requested on the forms listed in Section 1.5. In addition, in certain circumstances, name, address, phone number, SSN, DOB, and POB for the individual's immediate family members, former spouses, and cohabitants is also maintained, as well as information about others whom the individual identifies or who are identified by the investigator during the course of the investigation. Also, it contains information that is part of the subject's personal history.

The information that DMRS accesses in ESCS includes personally identifiable information about senior executives, including name, address, date of birth, sex, race, and ethnicity, as well as information about work experience, educational experience, salary, and awards.

2.2. What are the sources of the information and how is the information collected for the project?

The DMRS database is data extracted from the PIPS database, programmatically transformed during an extraction, transformation, and loading (ETL) process. ETL is a process in which data is delivered from the PIPS to the DMRS.

Additionally, the DMRS has read-only access to data contained in SBM, FTS, and ESCS and runs reports using that data as needed but does not store the information in the DMRS database.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, the DMRS does not use information from commercial or publicly available data sources.

2.4. Discuss how accuracy of the data is ensured.

The DMRS receives a copy of information from PIPS and does not independently verify its accuracy, nor does it independently verify the accuracy of the information it accesses in SBM, FTS, and ESCS. Information collected in the course of the background investigation is verified through review of corroborating records. The information may be checked by a group of reviewers who validate that the information is about the individual being investigated and is pertinent to the investigations process. The information may also be further scrutinized by a team of investigation case analysts who review the cases, validate, and verify responses from individuals. This team looks for anomalies or errors by reviewing the information obtained from third party sources and comparing it against information provided by the individual. Information in ESCS is checked for accuracy by the HR specialists at the agency that submits the information to OPM. Any inaccuracies that are identified are either corrected directly by the respective HR specialists or by contacting the ESCS administrators.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in DMRS may be inaccurate and result in inaccurate reports.

Mitigation: This risk is mitigated by obtaining daily data refreshes from PIPS of data that has been corrected in PIPS and by HR specialists checking their information for accuracy and correcting it as necessary.

Section 3. Uses of the Information

3.1. Describe how and why the project uses the information.

The DMRS uses the information it collects to support the NBIB management through reporting investigative information on items such as timeliness and workload for planning purposes. The reports that OPM ES generates through the use of DMRS to support its oversight function for the SES and to provide agencies transparency regarding their senior executives and Schedule C appointees.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

The DMRS is a tool to conduct information searches in an electronic data database. The reports resulting from searches can be pattern or anomaly analysis used to plan efficiencies in conducting investigations such as increasing or decreasing investigators in defined regions based on predicted workload.

3.3. Are there other programs/offices with assigned roles and responsibilities within the system?

Within OPM, only personnel and contractors who have a need for the information in the performance of their job duties have access to DMRS and the information contained therein. This includes authorized investigative

contractors, who have a need for the information in the performance of their investigative duties. DMRS users only have access to the particular information that is necessary to achieve their business function and the ESCS only has access to its assigned domain within the DMRS.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information in DMRS may be accessed or used inappropriately or in a manner not consistent with the original program's purpose or user's specific mission area and authority.

Mitigation: This risk is mitigated by creating dedicated user roles established by NBIB policy. Access controls permit access only to the minimum information that individuals need in the performance of their official duties. For example, an authorized user from OPMES is only able to access DMRS to view ECSC and run necessary reports; that same user cannot access the DMRS database containing all of the investigation information copied from PIPS, not run reports related to that information. DMRS users must have an account on opm.gov as well as a DMRS-specific account. Access is determined by NBIB access control and documented using Form 1665. In addition, system users are required to review the Rules of Behavior and received Annual Security and Privacy Awareness Training.

Privacy Risk: There is a risk that individuals who do not have a need to know the information in the investigative process will access the information.

Mitigation: This risk is mitigated by controlling who can access data and the type of data permitted to be seen. In addition, there are also built-in audit logs to monitor disclosures and determine who had access during this time. These logs are checked regularly to ensure that the system was is accessed appropriately.

Section 4. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The DMRS is not accessible by individual members of the public and, therefore, does not provide direct notice of its collection of information to individuals. However, subjects of investigations are provide notice, in the form of Privacy Act statements, at various points on information collection in the investigative process as are those whose information is contained in ESCS.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals do not have the ability to consent to the collection and use of their information in DMRS. However, individuals who are the subject of an investigation are notified at the point of collection, at the beginning of an in person interview, and on various consent forms about why their information is being collected and the purposes for which it will be used.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not receive adequate notice concerning how their information is used.

Mitigation: While individuals are not provided with notice specifically about DMRS, this risk is mitigated by the provision of Privacy Act Statements at various points of information collection. The Privacy Act Statement informs the individual on the uses of the information. While that statement does not explain the system specifically, it does provide information concerning how their information will be used. In addition, notification specifically about this system is provided through publication of this PIA.

Section 5. Data Retention by the project

5.1. Explain how long and for what reason the information is retained.

The DMRS follows the retention schedules identified in Section 1.4 of this PIA. The type of information and the associated action determine the specific regulatory retention periods.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be kept longer than is necessary to meet the business need of DMRS.

Mitigation: This risk is mitigated by adhering to the applicable records schedule so that records are not retained for longer than required.

Section 6. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

External agencies receive reports regarding their completed and outstanding investigations as well as reports concerning their senior executives and Schedule C appointees. Also, agencies contracted by NBIB to perform investigations receive status reports of outstanding investigations assigned to their agency.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing described above is compatible with the purpose for which the information was collected, which is, for the investigation information, in part, to provide investigatory information for determinations concerning whether an individual is or continues to be suitable or fit for employment by or on behalf of the Federal government or for military service, or whether an individual is or continues to be eligible for access to national security information. NBIB provides information to its customer

agencies so that they may make such determinations and provides information to others in order to collect all the information necessary to make those determinations. In addition, NBIB provides information to contractors who conduct the background investigations on its behalf. The OPM/CENTRAL 9 SORN contains routine uses that permit this sharing and are compatible with the original purpose for the collection. For the ESCS information, the external sharing is consistent with the purpose for which that information was collected, which is, in part, to assist OPM in carrying out its responsibilities related to the government-wide senior executive program. The OPM/CENTRAL 13 SORN contains routine uses that permit the sharing and are compatible with the original purpose for collection.

6.3. Does the project place limitations on re-dissemination?

Entities using NBIB systems are also governed by EO 13467, as amended by EO 13764, which allows agencies to release records within the agency and to store subject information for future reference. Each agency is required to ensure any re-disclosure of the information does not violate statutory, regulatory, or policy restrictions. NBIB background investigation records obtained from other agencies may include items that have been disclosed to NBIB with specific re-disclosure limitations. Agencies may coordinate this activity with the Bureau's Freedom of Information and Privacy Act office (FOI/PA) Office. External agencies that access DMRS reports through ESCS are required to sign a user access agreement which governs their use of the system.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The DMRS records to an audit log information such as who requested a report, the name of the report, and the date. The information recorded is for all users of the DMRS.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in DMRS, disclosed through a report, will be shared with a third party and used or disseminated

for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: The risk is mitigated by compliance with applicable documentation and through training regarding appropriate dissemination.

Section 7. Redress

7.1. What are the procedures that allow individuals to access their information?

Certain information contained in the DMRS and covered by the OPM/Central 9 SORN has been exempted from the access and amendment requirements in the Privacy Act. Individuals may request access to any non-exempt information by contacting FOI/PA, Office of Personnel Management, National Background Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618 or emailing FOIPARequests@nbib.gov. Individuals may submit their request by using form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, mailing address and email address (to receive materials electronically), any available information about the records being requested, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

Individuals can request access to their information that is covered by the OPM/CENTRAL 13 SORN by contacting the Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415-0001 and providing the following information: full name, Social Security number, and the address where employed.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Certain information contained in the DMRS and covered by the OPM/Central 9 SORN has been exempted from the access and amendment requirements in the Privacy Act. Individuals may seek to correct non-exempt information by contacting FOI/PA, Office of Personnel Management, National Background

Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618, in writing. Individuals may submit their request by using form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, precise identification of the records to be amended, a statement about and evidence supporting the reasons for the request, including all available information substantiating the request; mailing address and email address to which correspondence should be sent, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

Individuals can request that erroneous information that is covered by the OPM/CENTRAL 13 SORN be corrected by contacting the Office of Personnel Management, 1900 E Street, NW, Washington, DC 20415-0001 and providing the following information: full name, Social Security number, and the address where employed.

7.3. How does the project notify individuals about the

Individuals are notified concerning the procedures for requesting the amendment of records on the NBIB public website, https://nbib.opm.gov/foia-privacy-acts/requesting-an-amending-myrecords/#CopoyofBI, in the published OPM/CENTRAL 9 and OPM/CENTRAL 13 SORNs, and through this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to correct, access, or amend inaccurate information that is used by DMRS to generate reports.

Mitigation: This risk is partially mitigated by publishing clear instructions on the NBIB website, in the OPM/CENTRAL 9 and OPM/CENTRAL 13 SORNs, and in this PIA to inform individuals about how to access and request amendment to their records. Certain information is exempt from the access and amendment requirements of the Privacy Act; therefore individuals are not able to review or request amendment of that information.

Section 8. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in this PIA?

Role-based access controls are in place to restrict access to information in DMRS based on user role and need-to-know. The output media from the DMRS are predominantly reports delivered to a user's computer in the form of a spreadsheet or document.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM/NBIB employees and contractors, having access to the OPM LAN (network), are required to complete an annual IT Security and Privacy Awareness training. The DMRS system is only accessible through the OPM LAN; therefore, all DMRS users complete the annual training.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to any part of the system is approved specifically for, and limited to, users who have an official need to know the information for the performance of their investigative duties. Access is requested by submitting OPM 1665 "OPM IT Access Request Form" to NBIB Access Control officials who determine access to the system; the security office grants access based on need to know and business role.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The NBIB staff reviews MoUs and ISAs every three years for renewal or necessary adjustments. Any new access to the DRMS will be evaluated by the appropriate NBIB personnel and documented in a MoU or ISA, which is approved by the OPM Chief Information Security Officer (CISO). New uses of the information are business decisions determined by the NBIB Information Technology Management Office (ITMO), in coordination with relevant stakeholders.

Responsible Official

Charles S. Phalen, Director
National Background Investigation Bureau

Approval Signature

Signed Copy on File with the Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer