Privacy Impact Assessment
for the

Automated Record Checks International Justice and Public Safety Network (ARC-Nlets)

February 26, 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 ARC-Nlets system is to provide an automated workflow management tool solution for an interface between the International Justice and Public Safety Network (Nlets) and NBIB Automated Systems. This Privacy Impact Assessment (PIA) is being conducted because the ARC-Nlets system processes Personally Identifiable Information (PII) about candidates who are undergoing a background investigation and others whose information may be included in background investigation files.

Investigation Overview

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. 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, 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 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 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). 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 Automated Records Check – International Justice and Public Safety Network system (ARC-Nlets) is a commercial off-the-shelf product that was developed for NBIB as a workload management tool for users to process statewide law checks to the International Justice and Public Safety Network (Nlets). Nlets is a commercially available system that allows an NBIB investigation applicant's information to be retrieved from public records. The Nlets queries state criminal databases regarding the applicant's state criminal activity, if any. The use of commercial sources such as Nlets (and other publicly available National Agency Check (NAC) repositories) provides relevant data points to obtain a comprehensive picture of the applicants during the investigative process. ARC-Nlets maintains information pertaining to applicants who are the subject of an investigation while also enabling the electronic transfer of information between NBIB systems, and also out to Nlets. This system exists in paper form, but is more user-efficient, can process faster, and is more accurate in an automated electronic process. ARC-Nlets provides the automated ability to manage the query workflow, submissions, and reception of results from Nlets, with minimal human

intervention. This allows the NBIB staff to focus on analyzing results and expanding queries based on the results of the records check.

The system is also used as a central information portfolio that supports the implementation of investigations by facilitating the transfer of records information from Nlets to NBIB. This contributes to agencies having timely and sufficient information regarding credentialing, suitability, and/or security clearance determinations for their applicants. Automating the queries also provides the ability to increase the number of states, countries, and U.S. territories that can be queried automatically, which will decrease the time it takes to complete an investigation and help reduce any background investigations backlog.

The implementation of ARC-Nlets is also intended to eliminate the need to have paper documents move through the background investigation process, expending storage space, personnel resources, and money. Instead, information is routed electronically, eliminating the need for the repetitive printing of paper. This capability provides a computer-based logic to automatically process or update Nlets checks without the involvement of NBIB staff. The system routes only the Nlets checks that require human intervention and validation to NBIB staff, allowing an increased ability to track, audit and report on all Nlets queries.

The applicant information used in ARC-Nlets is routed through other NBIB systems. The Personnel Investigations Processing System (PIPS) allows for an automated entry, scheduling, case control, and closings of background investigations. It also stores the important information used in security and suitability programs and decisions. NFW is used to facilitate data exchange electronically with external agencies/organization for the NBIB. The ARC-Nlets system is the COTS product used to process information obtained from PIPS, and in turn transmits the information to external systems outside of OPM. Nlets is the product used to obtain publically available information for an individual.

The ARC-Nlets process begins when an investigation is scheduled in PIPS and an Nlets Statewide law enforcement item is created. Details from the item are passed from PIPS to NFW, which creates a request file that is sent to the ARC-Nlets system. ARC-Nlets in turn transmits the information to the

external Nlets system, which conducts a law enforcement records background check on the applicant. The results from the record check are then passed back to ARC-Nlets, then back to NFW, and ultimately back to PIPS. If there are documents that result from the records check that are relevant to the investigations, the records are sent to the OPM PIPS Imaging System (OPIS) system for retention. OPIS is the NBIB background investigation document repository system that retains images for applicant case files.

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, the NBIB 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.

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 ARC-Nlets is OPM/CENTRAL 9 Personnel Investigations Records which can be found at www.opm.gov/privacy.

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

Yes. The ARC-Nlets System Security Plan (SSP) was last updated on December 29, 2017 as part of the system's upcoming Authorization to Operate (ATO).

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

Yes, NARA General Records Schedule (GRS) 5.6 Security Records, items 170.

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 ARC-Nlets system is an automated system that does not collect information directly from individuals; therefore the Paperwork Reduction Act (PRA) does not apply. However, ARC-Nlets does collect and use some of the information that individual's record on the forms listed below that it obtains through other NBIB systems. The Office of Management and Budget (OMB) control numbers for the initial collections are:

Form Number	Form Name
SF-85	Questionnaire for Non-Sensitive Positions
SF-85P	Questionnaire for Public Trust Positions
SF-85PS	Supplemental Questionnaire for Selected Positions
SF-86	Questionnaire for National Security Positions

Form Number	Form Name
SF-86A	Continuation Sheet for Questionnaires
SF 85, SF 85P, AND SF 86	3206-0007

Section 2. Characterization of the Information

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

ARC-Nlets collects, uses, disseminates, and maintains information pertaining to applicants who are the subject of an investigation, including case specific information that is needed in order to process the statewide law check items, and additional subject data to include applicant name, address, phone number, aka name and date, Social Security number (SSN), date of birth, place of birth, height, weight, hair color, eye color, race, the position for which the applicant is being investigated, mother's full maiden name, current residence, offense related information, claimed residence at time of offense, and a flag indicating the applicant self-admitted an arrest.

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

The sources of information for ARC-Nlets are e-QIP, PIPS, and Nlets. Nlets is the commercially available system that allows an applicant's information to be queried from state criminal databases to determine an applicant's state criminal activity.

The applicant's data is initially entered in e-QIP via one of the forms listed in section 1.5 and transmitted to PIPS. Every night, PIPS sends information to ARC-Nlets via NFW regarding criminal history checks that need to be conducted. PIPS maintains the applicant's investigation file and, as the background investigation is being conducted, the investigation file in PIPS is monitored and updated by numerous stakeholders, including ARC-Nlets.

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

Yes. ARC-Nlets is a commercial off-the-shelf (COTS) querying application that interfaces with Nlets to query state criminal databases to determine if the applicant has any state criminal activity. Nlets, is a private not for profit corporation that links together and supports every state, local and federal law enforcement, justice, and public safety agency for the purposes of sharing and exchanging critical information.

Through the Nlets network, law enforcement and criminal justice agencies can access a wide range of information, from standard driver license and vehicle queries to criminal history and Interpol information.

ARC-Nlets receives criminal history data from the Nlets system, which is used to update the law enforcement item for the candidate's investigation within PIPS.

2.4. Discuss how accuracy of the data is ensured.

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 ARC-Nlets system staff specifically reviews the information from Nlets. Information such as full name, date of birth, and place of birth are analyzed to verify the information belongs to the proper applicant.

The ARC-Nlets process itself is an accuracy check to make sure the proper persons are affiliated with the proper data. 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.

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

Privacy Risk: There is a risk that the information obtained in the course of the investigation will be inaccurate resulting in an adverse decision for the individual being investigated.

Mitigation: This risk is partially mitigated by ARC-Nlets analysts reviewing the information from Nlets and validating applicant information by comparing basic data, such as name, social security number, and date of birth in the PIPS database. Prior to the information arriving in PIPS and during the collection of the data from the applicants, there are steps to validate that the data provided is appropriately formatted to meet NBIB's investigative needs. NBIB provides all applicants with formatting instructions and automatic format error messaging (during the collection) to ensure data is entered correctly. The applicants certify that their data is complete and accurate, to the best of their knowledge, before releasing the investigation request back to their sponsoring agency. The sponsoring agency is then responsible to check the accuracy of the data.

Privacy Risk: There is a risk that information obtained from commercial sources and electronic records searches will be misinterpreted or that relevant information may be overlooked, resulting in an adverse decision of the individual being investigated.

Mitigation: This risk is mitigated by reviewing and validating information received from PIPS. The ARC-Nlets system staff also reviews the information from Nlets to determine if it belongs to the applicant. The review is executed by ARC-Nlets staff that are trained in how to interpret the information they obtain in the course of the investigation and by having internal processes in place to validate the information. For example, a pre-review team validates the information for accuracy in the investigation against the PIPS data.

Section 3. Uses of the Information

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

Applicant information collected and processed in ARC-Nlets is used in order to request information about an applicant's criminal history, which information is in turn used by agency adjudicators to determine an individual's suitability/fitness for Federal employment and/or for eligibility and access determinations. Queries regarding the applicant are sent to Nlets, where the system responds with either a result of possible match or no record regarding the applicant's criminal history. If a possible match is found, the information is available to be reviewed to determine if the information belongs to the applicant. If it is the applicant, a determination is made on how to update the query. If it is not the applicant, the query will get updated to the classification "no record". If the search returns a "no record" result, the query is updated accordingly.

When determining how to update the query, many factors must be taken into consideration including questioning if the applicant listed the arrest when filling out the forms referenced in section 1.5. The system also helps NBIB staff determine what the applicant was charged with, and if or when an arrest took place.

Additionally, if an arrest is found on the applicant and the applicant did not admit to an arrest, it is considered material falsification and the item will be updated accordingly. Finally, if information on an arrest reported by the applicant is found, further work is required to obtain the arrest information outside of the Nlets search.

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.

No. The ARC-Nlets system does not use tools, programs or other technologies used to conduct electronic searches, queries or analyses.

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

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

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

Privacy Risk: There is a risk that authorized users may inappropriately disclose information in the system, either intentionally or unintentionally.

Mitigation: This risk is mitigated by subjecting all users to a background check, as well as through annual security and privacy awareness training.

There are also multiple layers of physical and technical protections that are used to safeguard the data. Physical security on the premises ensures that only authorized individuals have access to the building. Layered firewalls and data encryption methods ensure the data can only be accessed by individuals authorized by NBIB Access Control. This means, only authorized case managers can see the information assigned to them, based upon their authorization and privilege.

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 is accessed appropriately.

Privacy Risk: There is a risk that PII maybe 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 investigations policy. Access controls permit access only to the minimum information that individuals need in the performance of their official duties. PII stored or transferred must only be used in accordance with the investigative process. Measures that integrate administrative,

technical, and physical security controls place limitations on the collection of PII and protect PII against unauthorized disclosure, use, modification, or destruction. System users are required to review the Rules of Behavior and received Annual Security and Privacy Awareness Training.

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 ARC-Nlets system is an internal NBIB system that is not accessible by the public and/or individuals. Therefore, notice is not given to individuals by the system. However, subjects of investigation are provided notice, in the form of a Privacy Act statement, at the original point of the information collection, and again at the beginning of an in-person interview. They are also told they must provide true, complete, and correct information when completing forms and giving information to investigators and that failure to do so may delay the investigation or the adjudication of the case, and may raise questions concerning eligibility for a security clearance.

Notice is also given in the OPM/CENTRAL 9 SORN and in this PIA.

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

The ARC-Nlets system is an internal NBIB system that is not accessible by the public and/or individuals. Notice is not provided and consent is not obtained from individuals through ARC-Nlets.

Individuals receive Privacy Act statements at various points where information is collected directly from them. This informs them that providing information is voluntary but that if they do not consent to the collection of the required information, it may affect the completion of their background investigation. They do not have the ability, once they have agreed to the background investigation, to consent to some uses of their information and decline to consent to other uses. The exception to this is the SF86 Medical Release authorization, which is valid for 1 year from the date signed but can

be revoked at any time by writing to the U.S. OPM, preventing further collection of medical information covered by that form.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not receive adequate notice concerning how their information is being used and shared in ARC-Nlets.

Mitigation: This risk is mitigated by the provision of the Privacy Act Statement at the initial points of information collection from applicants and at the beginning of an in person interview. On forms and websites designed for collection for the NBIB investigations, (see question 1.5), the Privacy Act Statement informs the individual on the uses of the information. While that statement does not explain ARC-Nlets specifically, it does provide information concerning how their information will be used. In addition, notification about the information NBIB collects and uses is provided through publication of the OPM/CENTRAL 9 SORN and this PIA.

Section 5. Data Retention by the Project

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

The ARC-Nlets system retains an accounting of the investigative outreach, as well as any record that the data repository may return to the NBIB, following the retention schedule noted in Section 1.4. The ARC-Nlets system will retain queries and responses for 30 days after the law check request is closed and retains the transaction history for a minimum of one year.

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 for which it was collected.

Mitigation: This risk is mitigated by NBIB staff following the established retention schedule and documented guidance from NARA, which clearly defines retention requirements by record type and agency.

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.

Yes. ARC-Nlets shares case specific information that is needed in order to process the statewide law check item required for background investigations on applicants. ARC-Nlets enables the transfer of applicant information from PIPS, through NFW and finally to the external Nlets system. For each investigation request sent to ARC-Nlets, Nlets conducts a law enforcement records background check on each applicant, then passes the results or no-results back to ARC-Nlets for transmission back to PIPS through NFW.

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, 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 through ARC-Nlets to Nlets so that it may obtain information about applicants 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. These include Routine Uses (c) and (g) of the SORN, as follows:

(c) To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

(g) To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

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

ARC-Nlets data may only be disseminated for the purposes for which the data is authorized. NBIB is required to maintain a current list of law enforcement entities and other agencies for which NBIB is making the law enforcement query as well as the relevant contracts and memoranda of understanding. NBIB is prohibited from distributing data or statistics derived from data obtained from Nlets to anyone other than those contained on the list.

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

The ARC-Nlets system tracks disclosures by keeping a log of the activity within the system. These logs are reviewed by system administrators and can be accessed as needed to account for the disclosure of an individual's information. A response file is created when data is sent from ARC-Nlets to PIPS, or sent to NFW.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in ARC-Nlets 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: This risk is mitigated through training individuals with access to the system on appropriate use of the information and through establishing secure connections and role based access controls so that only authorized individuals and entities can obtain the information in the system.

Section 7. Redress

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

The ARC-Nlets system is an internal NBIB system that is not accessible by the public and/or individuals. Certain information contained in ARC-Nlets 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.

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

Certain information contained in ARC-Nlets 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.

7.3. How does the project notify individuals about the

While individuals from the public have no direct access to the information in the ARC-Nlets system, they are notified concerning the procedures for requesting the amendment of their investigation records on the NBIB public website, https://nbib.opm.gov/foia-privacy-acts/requesting-an-amending-myrecords/#CopoyofBI, in the published OPM/CENTRAL 9 SORN, 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 maintained by other agencies and shared to ARC-Nlets.

Mitigation: This risk is partially mitigated by publishing clear instructions on the NBIB website, in the OPM/CENTRAL 9 SORN, and in this PIA to inform individuals about how to access and request amendment to their records. Certain information is exempt from 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?

The NBIB system administrators, security administrators, IT specialists, and analysts have access to the system in order to perform their duties in managing, upgrading, and using the system. Role-based access controls are employed to limit the access of information by users and administrators based on the need to know the information for the performance of their official duties. The ARC-Nlets enforces separation of duties, preventing unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system.

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 ARC-Nlets are required to complete the annual IT Security and Privacy Awareness training.

In addition, the authorized users of ARC-Nlets receive training on how to process the statewide law checks using ARC-Nlets.

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

The ARC-Nlets system users are not authorized access to the system unless they have completed applicable training required to perform the responsibilities being requested for the ARC-Nlets system. Access to any part of the system is approved specifically for, and limited to, users who have an official need-to-know about the information for the performance of their investigative duties. NBIB access control officials determine access to the system and the security office grants access based on need to know and business role. In order to receive access, individuals must be U.S. citizens and undergo an appropriate background investigation.

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 the contracts, MoUs and ISAs every three years to renew and make any necessary adjustments. Any new access to the ARC-Nlets will be evaluated by the appropriate NBIB personnel and documented in a MoU or ISA, which is approved by the NBIB 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 Chief Privacy Officer

Kellie Cosgrove Riley
Chief Privacy Officer