

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

iComplaints Case Management System

Date: Monday, August 3, 2015

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

iComplaints Case Management System (iComplaints) is a cloud-based complaint management software that is offered as a Platform as a Service (PaaS) solution by MicroPact. MicroPact became certified as a Federal Risk and Authorization Management Program (FedRAMP) cloud provider in July 2014.

iComplaints maintains individual data records for all individuals who contact the Office of Small Business and Civil Rights (SBCR) to file informal and formal Equal Employment Opportunity (EEO) complaints. SBCR uses iComplaints to collect, track, and monitor EEO complaints in order to comply with Equal Employment Opportunity Commission (EEOC) data reporting requirements as set forth in the Code of Federal Regulations governing Federal Sector EEO complaint processing (29 CFR part 1614) and The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act).

2. What agency function does it support?

iComplaints supports SBCR in its mission to provide a work environment free of discrimination and retaliation in accordance with laws and regulations mandated by the No FEAR Act and enforced by the EEOC. iComplaints enables SBCR to do the following:

- *collect, track, and monitor complaint data*
- *ensure investigations are completed within mandated time-frames*
- *meet regulatory requirements to provide an annual Form 462 Report to the EEOC*
- *meet statutory requirements to provide an annual No FEAR Act Report to Congress*

- *conduct trend analysis on types of complaints in order to identify and eradicate discrimination in the NRC workplace, as well as report trends to relevant agency staff*

3. Describe any modules or subsystems, where relevant, and their functions.

Not applicable.

4. What legal authority authorizes the purchase or development of this system?

29 CFR part 1614 directs Federal agencies to process complaints of alleged discrimination under the laws enforced by the EEOC. As stated above, agencies must submit annual reports to the EEOC and to Congress, and they must purchase and/or develop systems that can compile the necessary information to track EEO complaint activity for case management and reporting as set forth in EEOC regulations.

5. What is the purpose of the system and the data to be collected?

In general, SBCR staff use the data that is collected and input into iComplaints to:

- *manage and track formal and informal EEOC complaints;*
- *review the status of open cases;*
- *analyze trends with EEO activity; and*
- *prepare and submit annual reports to Congress and to the EEOC.*

6. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Joel Kravetz	SBCR	(301) 415-0503
Technical Project Manager	Office/Division/Branch	Telephone
Richard Ousley	OIS	(301) 415-5220
Executive Sponsor	Office/Division/Branch	Telephone
Vonna L. Ordaz	SBCR	(301) 415-7380

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

- a. ___ New System X Modify Existing System ___ Other (Explain)

- b. **If modifying an existing system, has a PIA been prepared before?**

Yes as part of LEEs System

- (1) **If yes, provide the date approved and ADAMS accession number.**

ML081410105

- (2) **If yes, provide a summary of modifications to the existing system.**

Providing an individual PIA for IComplaints, it was previously part of the PIA done for LEEs System

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

- a. **Does this system maintain information about individuals?**

Yes.

- (1) **If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public).**

iComplaints maintains information concerning NRC staff, applicants for employment, former employees, and contractors who contact SBCR to file informal and formal EEO complaints.

- (2) **IF NO, SKIP TO QUESTION B.2.**

- b. **What information is being maintained in the system about an individual (be specific)?**

SBCR maintains the following information about individuals in the iComplaints system:

- *race*
- *color*
- *religion*

- *national origin*
- *gender, including transgendered status*
- *sexual orientation*
- *prior equal employment opportunity (EEO) activity*
- *age, including date of birth*
- *disability, including identifying physical or mental impairments*
- *grade/step/series/salary*
- *job title*
- *home address*
- *phone numbers*

SBCR also maintains the following complaint information in the iComplaints system:

- *name(s) of the alleged discriminating officials*
- *description of the complaint, including what the complainant considers to be discriminatory, such as:*
 - *denial of promotion or non-selection;*
 - *poor or negative appraisal;*
 - *denial of training;*
 - *harassment;*
 - *denial of reasonable accommodation; and*
 - *claims that genetic information was improperly revealed, obtained, or shared.*

c. Is information being collected from the subject individual?

SBCR staff collect information directly from subject individuals (i.e., aggrieved individuals and/or complainants), who contact SBCR to file informal and formal EEO complaints. SBCR staff then input the data into iComplaints.

(1) If yes, what information is being collected?

SBCR collects all of the information listed in Question B.1.b above.

d. Will the information be collected from 10 or more individuals who are not Federal employees?

Yes. Potential complainants include applicants for employment, former employees, and contractors.

(1) If yes, does the information collection have OMB approval?

The collection of information is mandated by EEOC regulations provided in 29 CFR part 1614.

(a) If yes, indicate the OMB approval number:

Not applicable.

e. Is the information being collected from existing NRC files, databases, or systems?

Yes.

(1) If yes, identify the files/databases/systems and the information being collected.

For complainants who are NRC employees, SBCR staff run demographic reports through the Federal Personnel and Payroll System (FPPS) to obtain information such as race, sex, age, disability, job series, grade, and step to compile a workforce profile about NRC workforces for investigations. FPPS is a system that is owned and authorized by the Department of the Interior (DOI). FPPS is interconnected with the Office of the Chief Financial Officer's (OCFO's) Human Resource Management System (HRMS). SBCR staff have been given access rights in order to gather data and run reports on NRC employees.

f. Is the information being collected from external sources (any source outside of the NRC)?

Yes.

(1) If yes, identify the source and what type of information is being collected?

Occasionally, when a complaint (formal or informal) is filed by a contract employee, SBCR will contact the contracting company to gather information, such as contact and cost information, to support the investigation/mediation process.

Additionally, a complainant may provide supporting documentation from outside sources such as a physician's medical report providing evidence of a disability, including the need for reasonable accommodation.

Further, if events related to a complaint occur outside of an NRC facility, then relevant records, such as travel or hotel receipts, phone records, or other kinds of evidence depending on the nature of the claims alleged by the complainant, are collected.

Hard copies of the supporting evidence are stored in a locked cabinet where only SBCR staff have access; soft copies of the supporting evidence are stored on a local, secure SBCR server, which is not a part of the iComplaints system authorization boundary.

- g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?**

Since much of the information is self-reported, SBCR does not question the accuracy of the data unless there is a reason to do so.

- h. How will the information be collected (e.g. form, data transfer)?**

SBCR collects information through both oral and written statements. During the informal complaint process, an EEO counselor gathers information either in person or over the telephone. The information is summarized and attached to a counselor's report. Like the supporting evidence, the counselor's report is stored in a locked cabinet where only SBCR staff have access and/or on a local, secure SBCR server, which is not a part of the iComplaints system authorization boundary.

In the formal complaint process, the individual completes and signs a formal complaint form, which is also maintained in the locked file cabinet and/or secure local server. The formal complaint forms are either mailed, hand delivered, faxed, or emailed to SBCR staff.

During the investigation, evidence and sworn statements from witnesses are gathered and compiled into a report, which is provided to the complainant and stored in the locked file cabinet and/or secure local server.

2. INFORMATION NOT ABOUT INDIVIDUALS

- a. Will information not about individuals be maintained in this system?**

No.

(1) If yes, identify the type of information (be specific).

- b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.**

Not applicable.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

SBCR uses iComplaints to manage and track complaint data in order to comply with EEOC regulatory requirements and No FEAR Act annual reporting requirements. SBCR compiles reports from the data maintained in iComplaints to identify trends, such as the number of complaints related to racial discrimination or the number of complaints related to sexual harassment. These reports enable SBCR to be proactive in eradicating discrimination in the NRC work environment.

SBCR also uses the data maintained in iComplaints to provide an annual Form 462 Report to the EEOC and to provide an annual No Fear Act Report to Congress.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes. Without the data maintained in iComplaints, SBCR would be unable to fulfill its mission to provide a work environment free of discrimination and retaliation, in compliance with EEOC laws and regulations and with the No FEAR Act. SBCR is able to submit the required annual report to Congress and the annual Form 462 Report to the EEOC more easily using the iComplaints system.

3. Who will ensure the proper use of the data in this system?

Civil Rights Program Manager Joel Kravetz will ensure the proper use of the data in iComplaints.

4. Are the data elements described in detail and documented?

Yes.

a. If yes, what is the name of the document that contains this information and where is it located?

SBCR generates reports from the data maintained in iComplaints. These reports include the following:

- *an annual Form 462 Report, which is submitted securely to EEOC*

Please note that when the Form 462 Report is submitted to the EEOC, it is redacted such that no PII is shown.

- *an annual No FEAR Act Report to Congress, which is publicly-available and does not contain PII*
- *reports of investigation issued the complainant and his/her attorney*
- *ad-hoc trend data, which may or may not contain PII depending on what data is requested as part of the ad-hoc report*

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

iComplaints aggregates the data into more usable formats such as tables and reports; iComplaints does not derive new data or create previously unavailable data.

a. If yes, how will aggregated data be maintained, filed, and utilized?

Aggregated data is used in investigations to determine whether discrimination occurred.

b. How will aggregated data be validated for relevance and accuracy?

Aggregated data is only gathered in an investigative file if the data could be relevant to prove or disprove discrimination. Since much of the information is self-reported, SBCR does not question the accuracy of the data unless there is a reason to do so.

c. If data are consolidated, what controls protect it from unauthorized access, use, or modification?

Role-based access control (RBAC) is implemented in iComplaints to control access to the system and to prevent unauthorized use. Roles are defined for each authorized user, which prevents authorized users from accessing other parts of the system. Users are strongly authenticated to the system. SBCR staff are the only authorized users of the iComplaints system.

The system logs unauthorized access attempts.

As previously stated, supporting documentation and evidence is stored in either locked file cabinets where only SBCR staff have access and/or the secure local SBCR server, which is not a part of the iComplaints authorization boundary.

Below is a list of the consolidated data and how it is protected:

- *Form 462 Report – Annual Form 462 reports are provided to the EEOC through a secure web portal, which is provided and managed by EEOC.*

- *Reports of Investigation – Once a Report of Investigation is issued to a complainant and/or to his or her attorney, the report is outside of SBCR’s control. SBCR informs all parties receiving the report that they are being provided Privacy Act protected materials and that they must safeguard the data or risk a Privacy Act violation.*
- *The No FEAR Act Report is publicly available, so access controls in this context do not apply.*

6. How will data be retrieved from the system? Will data be retrieved by an individual’s name or personal identifier? (Be specific.)

Information is retrieved by individuals name or case number

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No.

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

8. List the report(s) that will be produced from this system.

- *Annual 462 Report to EEOC*
- *Annual Report to Congress*
- *Ad hoc reports*

a. What are the reports used for?

SBCR submits the annual reports listed above to communicate the status of complaints brought against the agency. These reports also show NRC’s compliance with employment discrimination and whistleblower protection laws, in accordance with the No FEAR Act.

The ad hoc reports include compiled data about complaints on an as needed basis. For example, a particular office within NRC may request a report of all complaints filed by individuals in that office over the last 3 years; the report can be listed by the type of complaint.

b. Who has access to these reports?

The No FEAR Act Report (with summary statistical data but without PII) is posted to the NRC’s public website in accordance with Section 302 of the

No FEAR Act, which states that agencies must post data pertaining to formal complaints. Individuals who view the No FEAR Act Report include:

- *members of Congress;*
- *personnel from the EEOC, the Department of Justice (DOJ), and the Office of Personnel Management (OPM); and*
- *members of the public.*

The 462 Report, which is not publicly accessible, is provided to the Office of Federal Operations (OFO) under the EEOC through the EEOC Federal Sector EEO Portal (FEDSep).

Ad hoc reports are typically only provided to staff or management within SBCR; however, relevant staff within the Executive Director for Operations' (EDO's) office, the Office of the Chief Human Capital Officer (OCHCO), or the Office of the General Counsel (OGC) may have access and/or a need to know certain information contained in a report.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Only SBCR staff have access to the data in iComplaints.

(1) For what purpose?

SBCR staff use the data that is collected and input into iComplaints to:

- *manage and track formal and informal EEOC complaints;*
- *review the status of open cases;*
- *prepare and submit annual reports to Congress and the EEOC; and*
- *create ad-hoc reports as needed for statistical and/or trend analysis.*

(2) Will access be limited?

Access to the data in iComplaints is limited to SBCR staff with a need to know. The iComplaints administrator has limited access to some of the data such as case numbers; however, the administrator has no access to the PII data. OCHCO, OGC, and EDO staff with a need to know have access to ad hoc reports generated from iComplaints; however, only SBCR has access to iComplaints directly.

2. Will other NRC systems share data with or have access to the data in the system?

No other NRC systems have access to the data maintained in iComplaints.

(1) If yes, identify the system(s).

(2) How will the data be transmitted or disclosed?

3. Will external agencies/organizations/public have access to the data in the system?

Yes.

MicroPact support personnel serve as the system administrators. As a result, MicroPact personnel may obtain access to the data maintained in iComplaints while performing administrative functions on the system.

Reports generated from the data in iComplaints are provided to external organizations. The Form 462 Report is provided to the EEOC, the No FEAR Act Report is provided to members of Congress and to the Public, and reports of investigation are provided to complainants and/or to their attorneys.

(1) If yes, who?

- *MicroPact. MicroPact personnel may obtain access to the data in iComplaints while performing administrative functions.*
- *OFO/EEOC. EEOC staff have access to the Form 462 Report, which contains redacted information pertaining to formal and informal complaints filed against NRC. EEOC staff will also be provided with reports of investigation (ROIs) when appeals are filed by parties; however, EEOC staff do not have direct access to iComplaints.*
- *Congress and the Public. Congress and members of the public have access to view the annual No FEAR Act Report, which is mailed to Congress and posted to NRC's public website.*
- *Complainants and/or their attorneys. Complainants and/or their attorneys obtain ROIs, but do not have direct access to iComplaints.*

(2) Will access be limited?

Access to the data maintained in iComplaints is limited to SBCR staff.

Access to the Form 462 Report is limited to OFO/EEOC personnel, and access to reports of investigation are limited to the complainant and/or their attorneys. The No FEAR Act Report is publicly available, but does not contain PII.

MicroPact staff who may obtain access to sensitive data undergo background checks. MicroPact staff do not have user rights to the data and should not obtain access; however, as they act as the administrators for the system, access may be possible.

(3) What data will be accessible and for what purpose/use?

The No FEAR Act Report is a summary of statistical data pertaining to formal complaints and does not contain PII. ROIs include compiled data from the investigation and do contain PII.

The data provided in the Form 462 Report contains:

- the number of cases at different stages of the investigation process;*
- the EEO bases involved in each case;*
- the status of the cases, including findings of discrimination or no discrimination, for each case;*
- the costs associated with processing the cases, including settlements, investigations or other miscellaneous costs; and*
- data related to processing times (e.g., how long a case was in the informal complaint stage or how long an investigation took to complete).*

Note: *MicroPact personnel do not have a valid need-to-know for the PII data maintained in iComplaints; however, as MicroPact personnel serve as the administrators for the system, they may obtain access to the data.*

(4) How will the data be transmitted or disclosed?

The No FEAR Act Report is posted to the NRC's public website and is sent to Congress via regular mail. The 462 Report is provided to OFO/EEOC through the EEOC Federal Sector EEO Portal (FEDSep).

Transmission sessions are encrypted using secure sockets layer (SSL) v3.0 and transport layer security (TLS) v1.0.

E. RECORDS RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.

1. Can you map this system to an applicable retention schedule in [NUREG-0910](#), or the [General Records Schedules](#) at <http://www.archives.gov/records-mgmt/grs> ?

The records and information identified in the system are Federal records that are covered under General Records Schedule 1, Item 25a., EEO Records.

Disposition: Destroy 4 years after case closes.

- a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?
- b. If the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

The records and information identified in the system are Federal records that are covered under General Records Schedule 1, Item 25a., EEO Records.

Disposition: Destroy 4 years after case closes.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

No.

4. How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?

Data maintained in iComplaints is kept indefinitely and is never replaced.

5. What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?

Data maintained in iComplaints is kept indefinitely and is never deleted. Also, according to the MicroPact specifications, data cannot be overwritten.

6. Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?

None of the data or output from iComplaints is kept in ADAMS. As previously stated, the publicly-available No FEAR Act Report is posted onto the NRC's public website, and the Form 462 Report is submitted over a secure web portal provided by the EEOC.

7. **Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?**

iComplaints has the capability to delete records; however, it is SBCR's policy to keep all records since more data allows SBCR to produce more relevant and reliable trend analyses.

F. TECHNICAL ACCESS AND SECURITY

1. **Describe the security controls used to limit access to the system (e.g., passwords).**

The system administrator sets user rights and permissions, and assigns usernames and initial passwords.

To authenticate to the web server, authorized users must correctly enter their unique username and password, and use their NRC-provided PIV card. SBCR staff are the only authorized users of the iComplaints system. In addition, the system logs unauthorized access attempts.

As previously stated, supporting documentation and evidence is stored in either locked file cabinets where only SBCR staff have access and/or the secure local SBCR server, which is not a part of the iComplaints authorization boundary.

2. **What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?**

Only authorized personnel with a need to know will have access to the data maintained in iComplaints. Role-based access control (RBAC) is implemented in iComplaints to control access to the system and to prevent unauthorized use. Roles are defined for each authorized user, which prevents authorized users from accessing other parts of the system. In addition, MicroPact generates audit logs to determine if unauthorized access has occurred.

3. **Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?**

No.

(1) If yes, where?

4. **Will the system be accessed or operated at more than one location (site)?**

iComplaints is a web-based solution and can be accessed anywhere. The system is accessed via a secure website.

- a. **If yes, how will consistent use be maintained at all sites?**

Not Applicable.

5. **Which user groups (e.g., system administrators, project managers, etc.) have access to the system?**

Only the SBCR Civil Rights Program staff have access to iComplaints; however, MicroPact administrators may obtain access to the data while administering the system.

6. **Will a record of their access to the system be captured?**

Yes.

- a. **If yes, what will be collected?**

SBCR relies on MicroPact to regularly audit and review event logs.

7. **Will contractors be involved with the design, development, or maintenance of the system?**

Yes. MicroPact is an external service provider and is responsible for the development and maintenance of iComplaints.

In addition, SBCR employs a contractor who is responsible for inputting data into iComplaints.

8. **What auditing measures and technical safeguards are in place to prevent misuse of data?**

SBCR relies on MicroPact to employ auditing measures and technical safeguards to prevent misuse of data.

MicroPact software components (Windows, Tomcat, Oracle, and SQL Server) are configured to DISA Security Technical Implementation Guides (STIGs). . MicroPact is a FedRAMP-certified cloud provider.

9. **Are the data secured in accordance with FISMA requirements?**

Yes.

- a. **If yes, when was Certification and Accreditation last completed?**

MicroPact received its Authority to Operate (ATO) from the U.S. Department of Interior under FedRAMP on June 6, 2014.

MicroPact has also undergone numerous authorizations for Federal agencies based on security processes and guidance specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations."

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/CSD Staff)

System Name: iComplaints Case Management System

Submitting Office: SBCR

A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

This system contains personally identifiable information that is retrieved by individuals name and is currently covered under NRC's Privacy Act System of Records, NRC-9, "Office of Small Business and Civil Rights Discrimination Complaint Records."

Reviewer's Name	Title	Date
Sally A. Hardy	Acting Privacy Officer	August 17, 2015

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. _____

Comments:

The iComplaints system is a database that manages and tracks informal and formal Equal Employment Opportunity complaints for Federal employees, former employees and contractors. This is a system used to meet regulatory requirements to provide an annual report to Congress and an annual Form 462 report to the EEOC under the legal authority 20 CFR Part 16124. No OMB clearance is needed for this system.

Reviewer's Name	Title	Date
Fajr Majeed	Information Management Analyst	August 12, 2015

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

- No record schedule required.
- Additional information is needed to complete assessment.
- Needs to be scheduled.
- Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

The records and information identified in the system are Federal records that are covered under General Records Schedule 1, Item 25a., EEO Records. **Disposition:** Destroy 4 years after case closes.

If staff does not intend to follow this retention because it would like to retain the records or information indefinitely, then the records staff will need to work with them to understand their rationale and/or develop an appropriate retention schedule that would be applicable to these records. The records staff would then seek the approval of the National Archives and Records Administration for the new retention.

Reviewer's Name	Title	Date
Mary Haynes	Records Management Analyst	August 17, 2015

D. BRANCH CHIEF REVIEW AND CONCURRENCE

- This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.
- This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RA/
Date **8/18/2015**
Laura Pearson, Chief
FOIA, Privacy, and Info Collections Branch
Customer Service Division
Office of Information Services

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: Vonna L. Ordaz, Director, Office of Small Business and Civil Rights	
Name of System: iComplaints Case Management System	
Date CSD received PIA for review: August 5, 2015	Date CSD completed PIA review: August 17, 2015
Noted Issues: The records and information identified in the system are Federal records that are covered under General Records Schedule 1, Item 25a., EEO Records. Disposition: Destroy 4 years after case closes. If staff does not intend to follow this retention because it would like to retain the records or information indefinitely, then the records staff will need to work with them to understand their rationale and/or develop an appropriate retention schedule that would be applicable to these records. The records staff would then seek the approval of the National Archives and Records Administration for the new retention.	
Laura Pearson, Chief FOIA, Privacy, and Info Collections Branch Customer Service Division Office of Information Services	Signature/Date: /RA/ 8/18/2015
<i>Copies of this PIA will be provided to:</i> <i>John Moses, Director Solutions Develop Division Office of Information Services</i> <i>Kathy Lyons-Burke Senior IT Security Officer (SITSO) FISMA Compliance and Oversight Team Computer Security Office</i>	