Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Office of Civil Rights iComplaints

U.S. Department of Commerce Privacy Threshold Analysis

Office of Civil Rights/iComplaints

Unique Project Identifier: OS-061

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system*
The iComplaints system is a Major Application (MA).

b) *System location*
The system is primarily hosted in Sterling, VA, with a secondary site in Herndon, VA.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
The system does not share any interconnections with other DOC systems. Authorized system users access the iComplaints via their personal computer (PC) client (DOC-issued computers) Web browsers.

d) *The purpose that the system is designed to serve*
iComplaints is a commercial off the shelf web-based system used to support the Office of Civil Rights (OCR) and bureau Equal Employment Opportunity (EEO) offices in the entry, management and reporting of data related to EEO complaints. iComplaints has been operational since November 4, 2010. The information collected is personally identifiable information (PII) and business identifiable information (BII) for law firms, unions, and others who represent the complainants and contractors.

e) *The way the system operates to achieve the purpose*
iComplaints operates as a case management system. A typical transaction consists of entry and editing of case management information, i.e. dates and actions taken on the case, regulatory and internal due dates, OCR and Equal Employment Opportunity Commission (EEOC) case tracking numbers, names of OCR and bureau staff, and/or Office of the General

Counsel (OGC) attorneys and contractors assigned to specific case tasks, status and disposition of each complaint, and the names of contract firms assigned to case tasks, requisition numbers and contract costs.

Users access the DOC system via the DOC intranet. All the logic and processing functionality of DOC iComplaints resides on one or more central servers, with users accessing DOC iComplaints from their PC client Web browsers through the DOC iComplaints site. DOC iComplaints application users have no direct access to the DOC iComplaints Database.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

As noted above, the information collected includes PII and BII for persons, law firms, unions, and others who are complainants or who represent the complainants and contractors. EEO complaints are filed by employees of the Department and applicants seeking employment. PII includes contact information for the complainant (attorney/representative/union representative) and representatives (OGC's attorney assigned to the case) for either the complainant or the Department. Complainants also provide demographic and employment information relevant to his or her claim of discrimination.

BII maintained in the system contains contact information for law firms, unions and other agencies that represent each individual complainant. Other BII includes: name of the firm contracted to investigate the case, name and contact information of the assigned subcontractor, and the costs associated with the investigation.

g) Identify individuals who have access to information on the system

The system is accessible to authorized users within OCR and the bureau EEO Offices at National Institutes of Standards and Technology (NIST), National Oceanic Atmospheric Administration (NOAA) and Census Bureau on a role and official need-to-know basis only. Access is limited to EEO Managers, Specialists and Assistants assigned to perform case processing tasks.

h) How information in the system is retrieved by the user

As a case management system, information in the system may be retrieved by various fields included in the complaint case, including name of complainant, complaint case number, date of request, Bureau/Office, employee type, etc. Data is retrieved both manually for special requests and via reports generated automatically.

i) How information is transmitted to and from the system

Information is input manually by authorized users who access the system via Web application through DOC-issued computers. Data may be output in the form of reports or case files which are disseminated only within the framework of administrative complaint processes, and/or related litigation in federal court. Additionally, statistical reports may be generated from the system – these reports are provided annually to the EEOC, the Office of

Personnel Management (OPM), the Department of Justice (DOJ) and selected members of Congress in compliance with the No FEAR Act and the EEOC Form 462 Report.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption.

"Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the iComplaints system and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Jerry Beat

Signature of ISSO or SO: Larry J. Beat (Jerry) Date: 4/12/2019

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: JUN KIM Digitally signed by JUN KIM DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988 Date: 2019.04.30 14:50:47 -04'00' Date: _____

Name of Authorizing Official (AO): Terryne F. Murphy

Signature of AO: TERRYNE MURPHY Digitally signed by TERRYNE MURPHY DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=TERRYNE MURPHY, 0.9.2342.19200300.100.1.1=13001000472785 Date: 2019.05.23 10:19:35 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Wesley T. Fravel

Signature of BCPO: WESLEY FRAVEL Digitally signed by WESLEY FRAVEL Date: 2019.04.30 16:04:48 -04'00' Date: _____