Version Number: 01-2015

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
iComplaints System

Reviewed by: WESLEY FRAVEL Digitally signed by WESLEY FRAVEL Date: 2019.04.30 16:03:36 -04'00', Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2019.08.16 18:49:32 -04'00' effective 4/15/2019

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
OCR iComplaints

Unique Project Identifier: OS-061

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) a general description of the information in the system

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.

(b) a description of a typical transaction conducted on the system

Typical transactions are entries 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.

(c) any information sharing conducted by 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. Data uploaded can only be changed in accordance with the privileges provided by OCR. Access is limited to EEO Managers, Specialists and Assistants assigned to perform case processing tasks. The system provides a range of privileges established by the Program Administrators and include the visibility of data, read/write access, business rules, and administrator functions. Information within the system is also shared with the Employment and Labor Law Division, OGC, and other federal agencies (EEOC and the Merit Systems Protection Board) as required for case processing, but these entities do not have access to the system.

(d) a citation of the legal authority to collect PII and/or BII

The authority for processing discrimination complaints within the Department of Commerce is delegated to the Director, Office of Civil Rights, by Department Organization Order (DOO) 20-10. The Department's internal discrimination complaint program is described by Department Administrative Order (DAO) 215-9.

The authority for the Department's EEO complaint processing program is contained in the

regulations of the EEOC at 29 CFR § 1614, and policy guidance provided by EEOC Management Directive 110. Related laws and regulations governing the Department's authority to process complaints of discrimination include 42 U.S.C. 2000e-16; 29 U.S.C. 633a; 29 U.S.C. 791 and 794a; 29 U.S.C. 206(d); E.O. 10577, 3 CFR 218 (1954-1958 Comp.); E.O. 11222, 3 CFR 306 (1964-1965 Comp.); E.O. 11478, 3 CFR 133 (1969 Comp.); E.O. 12106, 44 FR 1053 (1978); and Reorganization Plan No. 1 of 1978, 43 FR 19807 (1978)

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

iComplaints is a moderate system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks.
__X__ This is an existing information system in which changes do not create new privacy risks.

(Check all that apply.)

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): PIA is updated to the new template format. There are no changes to the privacy risk/posture of the system.					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	x	e. File/Case ID	x	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	x
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSNs are no longer collected. The SSN field from the predecessor system was deleted during migration, but some records imported from the legacy system and retained for litigation holds may contain SSNs in text fields.

General Personal Data (GPD)					
a. Name	x	g. Date of Birth	x	m. Religion	x
b. Maiden Name		h. Place of Birth	x	n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	x
d. Gender	x	j. Telephone Number	x	p. Military Service	
e. Age	x	k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity	x	l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify): personnel actions and employment information as they relate to the matters underlying the complaint.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address		d. Queries Run	x	f. Contents of Files	x
g. Other system administration/audit data (specify):					

Other Information (specify)
Narrative information regarding claims of discrimination.
Costs associated with investigations.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	
Telephone	x	Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): DOC unions, if the union is representing an employee.					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	x	To promote information sharing initiatives	
For litigation	x	For criminal law enforcement activities	
For civil enforcement activities	x	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Regulatory reporting requirements -EEOC Annual Report of Complaint Activity; NoFEAR Act reporting (annual and quarterly)			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

EEO complaints are filed by employees of the Department and applicants seeking employment 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. This provides both parties (individuals working with the complainant and the. Department representatives) with the notices, reports, decisions, and supporting documents related to the complaint. A complainant is required to provide the demographic and employment information relevant to his or her claim of discrimination. This enables OCR to determine if the complaint meets procedural and/or jurisdictional requirements necessary to direct the scope of the investigation and adjudication of the complaint, which is directly related to OCR's core mission of enforcing nondiscrimination laws.

The BII maintained in the system contains contact information for law firms, unions and other agencies that represent each individual complainant. Other BII identifies the following: name of the firm contracted to investigate the case, name and contact information of the assigned subcontractor, and the costs associated with the investigation. This category of BII allows OCR to manage its investigative contracts to ensure costs allocated are controlled appropriately. Investigations contractors and subcontractors do not have access to iComplaints.
PII and BII are disseminated only within the framework of administrative complaint processes, and/or related litigation in federal court. Information is provided to the OGC's Employment and Labor Law Division, EEOC, Merit Systems Protection Board and/or Assistant U.S. Attorneys on a case-by-case basis. PII may also be shared with the servicing Human Resources Office (SHRO) to the extent required to carry out personnel actions ordered as corrective action, or the agreed terms for settlement.

Statistical data from the system is annually provided to the EEOC, the Office of Personnel Management, the Department of Justice, and selected members of Congress in compliance with the No FEAR Act and the EEOC Form 462 report.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		x
DOC bureaus	x		x
Federal agencies	x		
State, local, tribal gov't agencies			
Public			
Private sector	x		
Foreign governments			
Foreign entities			
Other (specify): DOC unions if union is representing the complainant	x		

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	X*		
Other (specify): "Contractors" refers to MicroPact Engineering, the vendor that hosts and maintains the system.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
x	Yes, notice is provided by other means.	Specify how: Notice is provided on form Complaint of Employment Discrimination Form (CD-498), which contains a Privacy Act notice. The information in iComplaints is directly provided from the claimant, on the above noted form, who files a complaint against the Department.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: The complainant can decline to provide PII/BII when he or she completes the CD-498.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The complainant provides consent when he/she completes and signs the CD-498.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may contact their servicing EEO Office or OCR for review and/or updates.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The system may only be accessed by authorized users entering a username issued by a program administrator and an encrypted password that must be changed every 90 days. Case visibility and read-write privileges are tailored to each user's bureau or office location and level of responsibility. The system also includes an "audit" capability that tracks change entries and edits by user, date, and time. Sessions terminate and users are automatically logged off if no activity occurs within 30 minutes.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 7/27/2018 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.

	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

iComplaints employs a thin-client implementation that requires no client-side support files. User access to the system is provided securely through web browsers. The browser supported by iComplaints IG is Microsoft Internet Explorer version 7.0 or higher and Firefox. Users access the DOC system via the DOC intranet. All of 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. On a network level, a user accesses the DOC iComplaints site (http://doc.icomplaints.com/). The web server is running on Windows is connected to an isolated firewall port in a DMZ. The firewall performs real-time, inline Antivirus and Intrusion Protection Systems on all traffic passing through it. The Apache server performs a redirect on the request and forwards the appropriate DOC iComplaints traffic back through the firewall to the Production environment. The DOC iComplaints application is stored on in an isolated Tomcat container running as its own service. Tomcat relays application requests to the Oracle Database server. Oracle then assigns a random Registered Port Number for the actual Database connection. DOC iComplaints application users have no direct access to the DOC iComplaints Database, all requests are made to the application, which verifies the integrity of the request and forwards to the database. Information then flows back out to the user, passing through the firewall twice before displaying in the local DOC intranet web browser.

The iComplaints system has a real-time backup/mirror of the database system from the primary site in Sterling, VA to the secondary site in Herndon, VA.

The iComplaints system database is also backed up to magnetic tape media fully once a week and incrementally once a day.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned

to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: EEOC GOV-1 https://www.gpo.gov/fdsys/pkg/FR-2002-07-30/pdf/02-18895.pdf and Commerce/Department 18 http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html .
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: NARA General Schedule 1
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing		Deleting	x
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

x	Identifiability	Provide explanation: Individual complainant information is identifiable and poses risks to integrity and confidentiality, leading to legal/financial exposure and risk to the Department's reputation.
x	Quantity of PII	Provide explanation: The volume of sensitive complaint information poses a substantial risk to the Department and individual complainants with respect to confidentiality and integrity, leading to legal/financial exposure and risk to the Department's reputation
	Data Field Sensitivity	Provide explanation:
x	Context of Use	Provide explanation: PII is used in the context of highly sensitive personal and workplace interactions, requiring preservation of confidentiality and integrity of the EEO process.
x	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act and EEOC regulations require OCR to preserve the confidentiality of EEO complaint information.
x	Access to and Location of PII	Provide explanation: EEO complaint information must be available on a strictly need-to-know basis.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
x	No, the conduct of this PIA does not result in any required technology changes.