Court Services and Offender Supervision Agency (CSOSA)

eComplaint
Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

August 30, 2021

Office of Equal Employment Opportunity, Diversity, and Special Programs
Court Services and Offender Supervision Agency
800 North Capitol St NW, Washington, DC 20002

POINTS OF CONTACT for eComplaint

Program Office Point of Contact: **Name: Denise Clark** **Title: Supervisory Attorney-Advisor Office: EEO/OD** **Phone: 202-442-1681** **Bldg./Room 800 North Capitol St. NW, room 745 Washington, DC 20002** **Email: Denise.Clark@csosa.gov**	**System Owner Point of Contact** **Name: Kathleen French** **Title: Senior Systems Specialist** **Office: OIT** **Phone: 202-585-7903** **Bldg./Room: 800 North Capitol St. NW, room 6313 Washington, DC 20002** **Email: Kathleen.French@csosa.gov**
Privacy Program Manager: **Name:** **Office:** **Phone:** **Bldg./Room** **Email:**	**Senior Agency Official for Privacy:** **Name:** **Office:** **Phone:** **Bldg./Room** **Email:**

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA.

Overview of eComplaint

The eComplaint is a system used by the Court Services and Offender Supervision Agency's (CSOSA) Office of Equal Employment Opportunity (EEO), Diversity, and Special Programs to track and report cases initiated through EEO complaint process. These cases are tracked through multiple phases including initiation, traditional counseling, Alternative Dispute Resolution (ADR), investigation, administrative judicial review, appeals, and final outcomes. The system is supported by CSOSA's Office of Information Technology (OIT). eComplaint collects personally identifiable information (PII) from cases initiated by CSOSA employees, former employees, and applicants against CSOSA staff.

To mitigate risks, eComplaint is a Federal Risk and Authorization Management Program (FEDRAMP) certified system and is locked down to allow access only through specific CSOSA Internet Protocol (IP) ranges.

The purpose of this Privacy Impact Assessment (PIA) is to address the privacy risks associated with the collection, use, maintenance, storing and disposal of PII in eComplaint.

1. Description of the System

1.1. Describe the system, including the system name, system, acronym, and a brief description of the major functions.

eComplaint is an automated EEO case management tracking system built on the eCase platform developed and hosted by AINS Inc. and supported by Tagence Inc. The system allows for the creation and management of records that track allegations of employment discrimination submitted by employees, former employees, and job applicants. It allows EEO staff to track the cases at the various stages of the EEO process. The system provides a means of swift but controlled collaboration and oversight between multiple users, simultaneously allowing for increased productivity while decreasing human error.

1.2. Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained, or shared.

Employees, former employees, and applicants for employment are protected by law to file complaints of discrimination based on one or more of the protected equal employment opportunity (EEO) bases. Each case must be investigated and each step of the complaint process must be tracked and completed within a specific timeline according to the standards set by the Equal Employment Opportunity Commission (EEOC). To carry out its functions, CSOSA's EEO office uses the eComplaint system to track and house supporting documentation for

discrimination cases. This system allows staff to electronically track and maintain information on the case and monitor the timeliness of processing each case.
CSOSA also has a legal obligation to report the total number of discrimination cases, the types of cases, the timeliness of the investigations, and the final outcomes to the Equal Opportunity Commission (EEOC), as well as to other federal entities with oversight responsibilities. eComplaint uses this data to generate reports, including the No Fear and 462 reports. This data is used by the EEOC, other federal entities, and the Agency for a variety of purposes, including monitoring and ensuring the Agency's accountability with the relevant laws, regulations, and directives.

1.3. Is this a new system or one that is currently in operation?

This is a new system.

1.4. Is this privacy impact assessment (PIA) new, or is it updating a previous version?

This is a new PIA.

1.5. Is the system operated by the agency, by a contractor, or both?

This system is operated by a contractor and it is hosted by AINS.

2. Legal Authorities and Other Requirements

2.1. What specific legal authorities and/or agreements permit and regulate the collection, and use of the data by the system?

Pursuant to 42 U.S.C. §§ 2000e-5(b), 42 U.S.C. §§ 2000e-16(a), (b) and (c) and 29 CFR 1614.102, this information is collected to create a factual record to adjudicate EEO complaints in a timely manner, order relief if appropriate and prepare reports mandated by the EEOC.

2.2. System of Records Notice (SORN) Requirement: Is the information in this system retrieved by a name or a personal identifier? If so, this system will need to be covered by a Privacy Act SORN.

The information in this system is retrieved by a name. For authorized users, the system uses a role based search, which determines which cases can be displayed.

2.3. Records Management Requirement: Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Yes. Records contained in this system are covered by NARA General Records Schedule (GRS) 2.3: Employee Relations Records.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timeliness in the records disposition schedule?

Yes, PII is disposed of in accordance with the approved NARA records schedule.

2.5. Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.).

Threats to privacy would be through compromise of the data in the eComplaint cloud service. This data breach could expose an employee's work and home phone numbers, email addresses, and physical address locations.

CSOSA's OIT uses a number of controls including splitting of roles involved with granting user access; strong passwords; the encrypted internet communication protocol; Hypertext Transfer Protocol Secure (HTTPS); Activity Directory authentication; transparent data encryption; encrypted data exchanges; and other procedural and system controls to ensure that database information is handled, retained, managed, and accounted for appropriately.

Potential privacy breaches are prevented and handled in three ways: CSOSA Information Technology equipment and procedures, the vendor's system equipment and procedures, and CSOSA's EEO policy and procedures.

eComplaint is authorized to operate in a federal environment by the Federal Risk and Authorization Management Program (FedRAMP). As such, it is in compliance with a set of comprehensive and rigorous information technology security requirements. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

3. Characterization and Use of Information

Collection

3.1. Select the specific personal information data elements (e.g. name, email, address, phone number, date of birth, social security number, etc.) that the system collects, uses, disseminates, or maintains.

Identifying Numbers					
Social Security		File/Case ID	X	Financial Account	
Taxpayer ID		Driver's License		Financial Transaction	
Employee ID		Credit Card			

Other identifying numbers (please specify):

General Personal Data					
Name	X	Date of Birth	X	Religion	X
Maiden Name		Place of Birth		Financial Information	
Alias	X	Home Address	X	Medical Information	X
Gender	X	Telephone Number	X	Military Service	
Age	X	Email address	X	Physical Characteristics	X
Race/Ethnicity	X	Education			
Other general personal data (specify): Disability DOB is only needed for age discrimination claims					

Work-related Data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	X
Work address	X	Business associates	X		
Other work-related data (please specify):					

Distinguishing Features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Video recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (please specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run		Contents of files	
Other system admin/audit data (please specify):					

3.2. Indicate the sources of the information in the system (e.g., individual, another agency, commercial sources, etc.) and how the information collected from stated sources (paper form, webpage, database, etc.).

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (please specify):					

Government Sources					
Within the Component	X	Other CSOSA components	X	Other federal entities	X
State, local, tribal		Foreign			
Other (please specify):					

Non-government Sources					
Members of the public	X	Public media, internet		Private sector	
Commercial data brokers					
Other (please specify):					

3.3. Where will the PII be stored in the system?

Data is stored in a SQL Database. The eComplaint hosted cloud based system is physically located at the AINS Headquarters.

3.4. Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exists in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.).

CSOSA selected the data set required to fulfil the requirement of tracking and responding to cases of discrimination. It was decided that requiring a social security number was an unnecessary risk and not needed to complete our requirements so it was decided that a unique identifier would be used in this field instead. The data gathered is done through the EEO process which is either face-to-face, email or regular mail. Only certain EEO Staff have access to this system and the few staff that have access outside of EEO have been limited due to the confidential nature of the data. Data is gained from outside sources; however, it is not a direct electronic transfer, instead, as part of the EEO Process, interviews are conducted and documented. This information is uploaded to the system only by identified EEO staff. Although part of the process includes alternative dispute resolution (ADR), the staff which perform ADR are not always EEO staff, so any information on this process is documented and sent to EEO Staff to upload to the eComplaint system.

Purpose and Use of the System

3.5. Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The eComplaint system is used to collect information regarding EEO discrimination

cases initiated by Agency employees, former employees, and applicants against the Agency. Once a complainant initiates a claim of discrimination through fax, email or by phone, an EEO Office employee logs into eComplaint using their login credentials. If this is an initial contact, the EEO staff will create a new Complainant profile in the system using PII. Otherwise, the EEO staff member retrieves case data including PII, case status and details of the complaint based on the complainant's name or case number. The EEO Employee then inputs new information about the discrimination case into the eComplaint database. Periodically, the EEO staff run a report to generate a summary of these discrimination cases and exports the reports, saves the information to a secure network drive, and sends the reports to the EEOC and other federal entities with oversight authority.

3.6. Select why the information in the system is being collected, maintained, or disseminated.

Purpose			
For criminal law enforcement activities		For civil enforcement activities	
For Intelligence activities		For administrative matters	
To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives	
To conduct analysis to identify previously unknown areas of note, concern, or pattern		For administering human resources programs	
For litigation			
Other purpose (please specify): To fulfill legal mandates and to enable the Agency to monitor its compliance with EEO directives and its own goals.			

Social Security Numbers

3.7 Does they system collect Social Security Numbers?

No.

3.8 Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

N/A.

4. Notice

4.1. How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The system itself does not provide a privacy notice. However, a Privacy Act Statement is sent to the complainant through email, mail, and/or handed to complainant in person. This Notice lets the person know that PII will be collected during the complaint process.

If the person does not wish for this information to be collected they cannot opt out, though they may exercise their option not to pursue this avenue of complaint.

4.2. Provide the text of the notice, including where it can be found, or the link to the webpage where notice is posted.

Authority:

Pursuant to 42 U.S.C. §§ 2000e-5(b), 42 U.S.C. §§ 2000e-16(a), (b) and (c) and 29 CFR 1614.102, this information is collected to create a factual record to adjudicate EEO complaints in a timely manner, order relief if appropriate and prepare reports mandated by the EEOC.

Purpose: Information is collected to track equal employment opportunity (EEO) cases and enable contact with the Agency employee, former employee, or applicant initiating the EEO process.

Routine Use:

Information may be disclosed for any of the following reasons:

- *For Law Enforcement Purposes*: To disclose pertinent information to the appropriate Federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation or order, where CSOSA becomes aware of an indication of a violation or potential violation of a civil or criminal law or regulation.
    - *For Litigation*: To disclose information to the Department of Justice for the purpose of representing CSOSA, or its components or employees, pending or potential litigation to which the record is pertinent.
    - *For Judicial/Administrative Proceedings*: To disclose information to another Federal agency, a court, grand jury, or a party in litigation before a court or administrative proceeding being conducted by a Federal agency, when the Federal Government is a party to the judicial or administrative proceeding.
    - *For National Archives and Records Administration*: To disclose information to the National Archives and Records Administration for use in records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
    - *For Congressional Inquiry*: To provide information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
    - *For Data Breach and Mitigation Response*:

- To provide information to appropriate agencies, entities, and persons when (1) the CSOSA suspects or has confirmed that there has been a breach of the system of records; (2) the CSOSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the CSOSA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the CSOSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- To provide information to another Federal agency or Federal entity, when CSOSA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach, or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosures: Disclosures are voluntary; however, failure to provide the information may delay or prevent the processing of an EEO matter.

4.3. What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of this system/project?

During initial inquiry, when the Privacy Act Notice is sent or read to them, the individual can opt out including initiating a pre-complaint. In that case, no PII will be collected.

5. Information Sharing

Internal

5.1. How do agency personnel gain access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, etc.)?

CSOSA staff and contractors must have an internal Active Directory network Login ID account before access can be granted. Then, in order to acquire access to eComplaints, they must submit a request ticket through our OIT Customer support desk. This request goes to the IT Admin for eComplaints. The administrator then verifies with the EEO Director that the staff should be granted access.

5.2. Will information be shared internally with other CSOSA program offices and/or components, if so, which ones?

Yes, information will be shared with the Office of General Counsel and the Office of the Director.

5.3. What information will be shared and with whom?

The only information shared with the Office of General Counsel and the Office of the Director is the complainant names and the status of the complaints.

5.4. How will the information be shared?

EEO staff members summarize data into a manually created chart, including names, and case statuses.

5.5. What is the purpose of sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

This information is shared to enable the Agency to track its compliance with the EEO laws, regulations, and directives as well as in furtherance of the Agency's objective of creating and maintaining a workplace free of discrimination, harassment, and retaliation.

5.6. Describe controls that the program offices and/or components have put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information.

CSOSA requires employees to complete mandatory IT Security Awareness Privacy, and Records Management training, both of which have sections on the proper handling, retention, and disposition of information, including PII. Additionally, within the eComplaint system, audit logs are available for review.

5.7. Is the access to the PII being monitored, tracked or recorded?

The system has an audit log that can be used to run reports on individual users' access to and actions within the system.

External

5.8. Will the information contained in the system be shared with external entities (e.g. another federal agency, District of Columbia agency, etc.)?

Yes, however, no PII data is shared with external agencies. Summary statistical data, such as number of cases, types of cases, timeliness of investigation, and

final outcomes is shared with the Equal Employment Opportunity Commission (EEOC) in the form of the 462 report and No Fear reports. These reports provide statistical data only and do not include any individual data.

5.9. What information will be shared and with whom?

Summary report data is shared with the EEOC and other federal entities, certain members of Congress, the Office of Personnel Management, and the Attorney General. As required by law, the Agency makes these reports accessible to the public. These reports include the EEOC's mandatory 462 and No Fear reports. These reports include the total number of cases, the number of cases by bases and issues, the timeliness of investigations, and the outcomes.

5.10. What is the purpose of sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

CSOSA shares the specified information with the external entities that have oversight responsibilities, as noted in section 5.9. This information is compiled and tracked to monitor and ensure the Agency's accountability with the relevant laws, regulations, and directives.

5.11. Is the system able to provide an accounting of disclosures?

The system has an audit log that can be used to run reports on individual users' access to and actions within the system.

5.12. What controls are in place to prevent the misuse (e.g., browsing) of data by authorized users who have access to the data?

Controls in place to prevent the misuse of data by authorized users with access to the data include Least Privilege and Separation of Duties.

Least privilege is a technique that restricts data access rights for applications, servers, etc. to only those permissions absolutely required to perform authorized and necessary operational or maintenance activities.

Separation of duties is a classic information security method to manage conflict of interest, the appearance of conflict of interest, and fraud by restricting the amount of power held by any one individual.

eComplaint has multiple layers of security that protect content to the object level and can be applied to a user, group of users, or set as a general feature. Account access within the system is also limited in that users have a defined time period during which their access is actually active. This automatic feature will log out inactive users and disable their user account based on their access needs. The system can generate both

usage and customized access reports that will report users who have been inactive or disabled from the system as needed.

Additionally, the audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records training requirements help prevent unauthorized access to data, browsing and misuse.

5.13. Is there a way to identify unauthorized users? If so, what controls are in place to prevent a data breach?

Each user has unique credentials and access and data changes are logged. The risk of a data breach is minimized through the use of auditing control. An example of an auditing control would be the ability of an authorized account administrator to review the database to look for abnormal activity, such as odd-hour attempts at database querying. Access controls prevent an unauthorized user from logging in and gaining access to the system. Additionally, non-administrative users can only access their own data.

5.14. Does the agency provide annual security and privacy training for agency employees and contractors?

Yes, the Agency provides annual security and privacy training. IT security training is covered in the Agency's annual IT Security Awareness training that is required for all CSOSA staff. Annual Privacy Training is also required.

5.15. Who is responsible for assuring safeguards for PII in the system?

The system administrator and all users of the system, including the AINS hosting staff and Tagence developers, are responsible for ensuring the correct use and safeguarding of PII.

5.16. How will owners of the PII be harmed if privacy data is unlawfully disclosed?

If information is unlawfully disclosed, individuals could be harmed by identity theft, embarrassment or blackmail.

5.17. If contractors have access to the system, has the Agency provided the contractor, who works on the system, a confidentiality agreement or a Non-Disclosure Agreement (NDA)?

Yes, contractors are all required to sign and complete an NDA before starting employment with or on behalf of CSOSA and gaining access to the data and/or system.

5.18. What other IT security measures has the Agency implemented to protect PII in the system?

There are no other IT security measures outside of what has already been discussed.

6. Auditing and Accountability

6.1. How does the system owner ensure that the information is used in accordance with the stated practices in this PIA?

The system owner ensures that the information is used in accordance with the stated practices by ensuring that all employees are made aware of their responsibility to protect and safeguard all PII, annual security and privacy training, and the completion of an annual third-party risk management assessment of the system.

6.2. What are the privacy risks associated with this system and how are those risks mitigated?

The privacy risks are the same as the threats to privacy as outlined in the responses to Question 2.5 and Question 3.4:

- Collection of inaccurate information: This is mitigated by the use of source documents for collecting and entering the information
- Mistakes in data entry: This is mitigated by confirming with complainant at the time of submission of the complaint to verify PII.
- Exposure of PII to unauthorized persons: This is mitigated by requiring paper records to be secured in an employee's desk or in the unit's secured file room when not in use. Staff members at CSOSA are required to complete Records Management, Privacy Awareness, Ethics, and Information Security Awareness training on a periodic basis.
- Collection of extraneous information: This is mitigated by limiting the PII collected in eComplaints to what has been authorized in law and regulations or OGC. Collection of information required solely for matching eComplaints is limited to those identifiers that best identify the complainant, or as required by law and/or regulation.
- Vulnerabilities in system access and exchanges: This is mitigated by employing Federal Government standard/approved technical controls to ensure data is protected while stored and exchanged in the eComplaint system of records. Reference Operational Instruction OIT-2019-01-01 for Computer access controls put in place. This policy can be found on the CSOSA Intranet here: https://intranet.csosa.gov/OperationalInstructions/OIT-2019-01-01-Access-Controls.pdf
- Audits of eComplaints by third parties (e.g. annual FISMA audit, annual financial audit), completed as scheduled by CSOSA Office of Information Technology, mitigate risk through external review of the system and associated procedures for data handling and risk mitigation.

7. Data Quality and Integrity

7.1. How will the information that the Agency collects be verified for accuracy and completeness when it is entered into the system?

PII accuracy and completeness is verified by the EEO staff during the initial inquiry.

7.2. Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will CSOSA mitigate these risks?

Risks dealing with data quality and integrity include complainants supplying incorrect data or system users inputting incorrect information. Staff must rely on complainants providing accurate data, and validate it by confirming with the complainant.

8. Privacy Policy and Statement

8.1. Has the agency provided a privacy statement or policy for this system and is it provided to all individuals whose PII is collected, maintained or stored?

Yes.

8.2. Is the privacy policy publicly viewable? If so where?

Yes, the privacy policy is provided at: https://www.csosa.gov/privacy-policy.

Authorizing Signatures

This Privacy Impact Assessment has been conducted by Denise Clark and has been reviewed by Sheila Stokes, the Senior Agency Privacy Official, for accuracy.

Denise M. Clark

System Owner Name (Please Print)

Denise M. Clrk — August 30, 2021

System Owner Signature — Date

Willis Stamps

Privacy Program Manager Name (Please Print)

Willis J. Stamps II — 08/30/2021

Privacy Program Manager Signature — Date

Sheila Stokes

Senior Agency Official for Privacy (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.08.30 14:35:12 -04'00'

Senior Agency Official for Privacy Signature — Date