



Department of Energy

WingSwept OCR-EEO Case Management and Tracking System (CMTS)

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	02/16/2023	
Departmental Element & Site	Department of Energy (DOE), Office of the Chief Information Officer (OCIO), Cybersecurity Compliance and Oversight Office, (IM-32)	
Name of Information System or IT Project	WingSwept Case Management and Tracking System (CMTS) (OCR-EEO)	
Exhibit Project UID	N/A	
New PIA <input checked="" type="checkbox"/>	New PIA	
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	Patricia Zarate (SO)	202-586-2248 patricia.zarate@hq.doe.gov
Local Privacy Act Officer	Brooke Dickson (LPAO)	202-287-5786 Brooke.Dickson@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	George Hughes (ISSO)	917-637-0622 George.hughes@hq.doe.gov
Person Completing this Document	George Hughes (ISSO)	917-637-0622 George.hughes@hq.doe.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

Purpose of Information System or IT Project

The Office of Civil Rights and Equal Employment Opportunity (OCR-EEO) will use the Case Management and Tracking System (CMTS) for two major program areas: equal employment opportunity (EEO) complaints processing and external civil rights enforcement activities.

EEO complaints processing includes entering and retrieving information or documents compiled during the informal EEO complaint stage and formal EEO complaint stage, including, but not limited to: EEO counseling, investigations, notices, final agency decisions, and U.S. Equal Employment Opportunity Commission (EEOC) hearings and appeals of complaints filed under Title VII of the Civil Rights Act of 1964, Age Discrimination in Employment Act, Section 501 of the Rehabilitation Act, the Genetic Information Nondiscrimination Act, the Equal Pay Act, and related statutes, regulations, executive orders, and other legal authorities and directives. CMTS will provide similar functionality as our legacy platform for EEO Complaints, which is called iComplaints, but it will also provide additional capabilities regarding workflow, customizable reports, and document creation, editing, and storage (potential records storage). The system will contain information regarding employees, former employees, applicants for employment, and any individuals who raise EEO complaints. It will also include some information regarding witnesses and management officials involved in EEO investigations. The system will collect and maintain information/data for all informal and formal EEO complaint processing, monitoring, and tracking, including complaint contact information (name, address, email address, phone number), complaint claims and bases, documentation supporting complaints (including, in some cases, date of birth and/or disability), complaint notices and communication (e.g., EEO counselor’s report, notice of right to file, rights and responsibilities, formal complaint, accept/dismiss letter, etc.), investigation documentation (e.g., investigation request letter, investigation plan, amendment approval/denial, evidence collected from relevant sources, affidavits, report of investigation, etc.), hearing documentation, appeals documentation, and compensatory damages documentation.

External civil rights activities are those mandated by civil rights obligations for programs receiving Federal financial assistance (FFA) pursuant to Title IX of the Education Amendments of 1972, Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, Title VI of the Civil Rights Act of 1964, and a related statutes, regulations, executive orders, and other legal authorities and directives. CMTS will maintain information on: (1) Individuals affiliated with FFA applicants and FFA recipients, subrecipients, licensees, and contractors; (2) Individuals who apply to, participate in, benefit from, or are otherwise engaged with programs or activities operated by FFA applicants and FFA recipients; (3) Complainants, subjects, victims, witnesses, parents/legal guardians, advocates, and/or other representatives; and (4) Individuals to whom the Department provides technical assistance, among other potential individuals and/or entities.

With respect to external civil rights activities, CMTS will also collect and maintain information related to complaints, pre-award reviews, complaint investigations,



MODULE I – PRIVACY NEEDS ASSESSMENT

compliance reviews, and technical assistance, for which, information about individuals includes, but is not limited to: full name, street address, telephone number, email address, academic record, employment record, occupational status, demographic data (race, color, national origin, sex, disability, age), parental/marital status, household/housing status, income level, and energy access.

Information maintained within CMTS will be obtained directly from publicly available sources, DOE employees or contractors, other Federal agencies, individuals on whom it is maintained, and/or from the parents/legal guardians, legal representatives, or advocates thereof, and/or participants, candidates, beneficiaries, licensees, contractors, and third parties engaged with programs and activities operated by any entities that may receive FFA from the Department, among other potential individuals and/or entities. Information is also obtained directly from entities (FFA applicants and FFA recipients), which can include an instrumentality of state or local government, institution of higher education, corporation, partnership, sole proprietorship, other private organization, or any combination thereof.

Type of Information Collected or Maintained by the System:

- SSN
- Medical & Health Information (related to disability claims and/or reasonable accommodation claims)
- Financial Information (related to compensatory damages, etc.)
- Clearance Information
- Biometric Information
- Mother's Maiden Name
- DoB, Place of Birth (related to Age Discrimination in Employment Act claims)
- Employment Information
- Criminal History
- Name, Phone, Address
- Other – Please Specify



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>Has there been any attempt to verify PII does not exist on the system?</p> <p><i>DOE Order 206.1, Department of Energy Privacy Program, defines PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.</i></p>	N/A
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	The system will contain PII.

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	YES
<p>2. Is the information in identifiable form?</p>	YES
<p>3. Is the information about individual Members of the Public?</p>	YES
<p>4. Is the information about DOE or contractor employees?</p>	<p>YES</p> <p><input checked="" type="checkbox"/> Federal Employees</p> <p><input checked="" type="checkbox"/> Contractor Employees</p>

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE



MODULE II – PII SYSTEMS & PROJECTS

1. AUTHORITY

What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?

EEO Complaints Processing: This information is required for the management and tracking of EEO complaints pursuant to U.S. Equal Employment Opportunity Commission (EEOC) regulations at 29 C.F.R. Part 1614, EEOC Management Directives 110 and 715, and the EEOC annual 462 Report. The 462 Report provides an overview of a Federal agency’s EEO complaint activity by fiscal year, and the data maintained in the WingSwept CMTS will be utilized to develop the Department’s annual 462 Report. In addition, the Elijah E. Cummings Federal Employee Antidiscrimination Act of 2020 (Cummings Act) (Pub. Law 116-283), requires Federal agencies to maintain an EEO complaint tracking system. Furthermore, the No FEAR Act requires Federal agencies to publish quarterly EEO complaint data and an annual No FEAR Act Report, and the data maintained in the WingSwept CMTS will be utilized to satisfy the No FEAR Act data requirements. Based on these statutory and regulatory requirements, the EEO case tracking system must be able to accurately identify the individual making the complaint and to ensure that the EEO case information is accurate and up to date. Finally, the Department is responsible for implementing the following civil rights statutes that prohibit discrimination in the workplace, which OCR-EEO implements through the EEO complaint process: Title VII of the Civil Rights Act of 1964, Section 501 of the Rehabilitation Act, the Age Discrimination in Employment Act, the Genetic Information Nondiscrimination Act, and the Equal Pay Act.

External Civil Rights Activities: OCR-EEO implements external civil rights compliance and enforcement activities, in relation to recipients of DOE federal financial assistance, pursuant to Title IX of the Education Amendments of 1972, Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, Title VI of the Civil Rights Act of 1964, and a variety of related statutes, regulations, executive orders, and other legal authorities and directives, including the Department’s external civil rights regulations at 10 C.F.R. Parts 1040, 1041, and 1042. It is a requirement that the system be able to accurately identify an individual making a complaint and that this information is accurate and up to date.



2. CONSENT

What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?

EEO Complaints Processing: Both the EEO Pre-Counseling Intake Form, which an aggrieved individual must submit to initiate the informal EEO complaint process, and the Formal Complaint of Discrimination Form, which an aggrieved individual must complete to file a formal EEO complaint, inform those individuals utilizing the EEO process that the Privacy Act is applicable to the EEO process. At the informal stage of the EEO process, an individual may request anonymity during the EEO counseling process, pursuant to EEOC regulations found at 29 C.F.R. Part 1614. However, an individual who requests anonymity at the informal stage of the EEO process must still fully complete and sign the EEO Pre-Counseling Intake Form. In addition, the individual's name and complaint information will still be included in the CMTS system. Anonymity is not permitted at the formal stage of the EEO process, pursuant to EEOC regulations found at 29 C.F.R. Part 1614.

The regulations do not contain a provision permitting a complainant to decline to have their complaint information maintained in a case management/tracking system.

External Civil Rights Activities: The OCR-EEO webpage informs individuals that an external civil rights complaint should contain the following information:

- your name, address, and telephone number;
- the name and address of the agency, institution, or department you believe discriminated against you;
- how, why, and when you believe you were discriminated against, including as much information as possible about the alleged acts of discrimination, and the names of the individuals whom you allege discriminated against you, if known; and
- the names of any persons, if known, that the investigating agency could contact for additional information to support or clarify your allegations.

DOE external civil rights implementing regulations found at 10 C.F.R. Section 1040.104(c)(2) inform potential complainants that if a complaint is accepted for investigation, the investigation will ordinarily be initiated by a letter requesting data pertinent to the complaint and advising the recipient of DOE financial assistance of: the nature of the complaint, and with the written consent of the complainant, the identity of the complainant. However, the regulation also provides that in the absence of the complainant's consent to release his/her/their identity, OCR-EEO may determine that the release of the complainant's identify is necessary to address/resolve the complaint.

The regulations do not contain a provision permitting a complainant to decline to have their complaint information maintained in a case management/tracking system.



MODULE II – PII SYSTEMS & PROJECTS

<p>3. CONTRACTS</p> <p>Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?</p>	<p>Yes. Contractors with WingSwept developed and configured CMTS for OCR-EEO. On p. 52 of the Agreement with WingSwept, its reads:</p> <p>(2) Access to and use of information.</p> <p>.....</p> <p>(ii) In addition, the Contractor agrees that to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. 552a), or other confidential or privileged technical, business, or financial information under this contract, it shall treat such information in accordance with any restrictions imposed on such information.</p> <p>.....</p>
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>CMTS poses a serious privacy risk to individuals in light of the potentially sensitive information contained in the complaint process. CMTS will have no greater impact upon individuals' privacy than the current legacy system for EEO Complaints processing (iComplaints). Should sensitive PII be compromised, it could cause personal, professional, and social harm to individuals which may include financial harm and embarrassment. The existence and content of complaints constitute sensitive PII which could significantly impact individuals' professional status or reputation.</p> <p>The system observes protections in contemplation of the Fair Information Practice Principles (FIPPs) to mitigate privacy risk. Individuals choose which information to provide with their complaints in furtherance of individuals participation and data minimization. Individuals are provided with case status notifications throughout the process to promote transparency. PII related to external civil rights complaint and compliance activity is maintained on DOE network drives used only for explicitly authorized purposes relating to complaints processing in furtherance of use limitation and purpose specification. Data quality is confirmed through the investigation process. A series of administrative and technical controls are implemented to protect individuals and their data.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Yes, PII can be retrieved by an identifier. Users will be able to retrieve cases by individuals' names, among other identifiers (e.g., case numbers, stage of case processing, bases alleged, issues alleged, and other data fields that will be maintained) if they file EEO complaints or initiate external civil rights complaints with OCR-EEO.</p>
<p>6. SORNs</p> <p>Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>?</p> <p>If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>EEO Complaints Processing: Yes. A government-wide SORN for EEO Complaints processing, entitled "EEOC/GOVT-1," has been published at 81 FR 81116 (Nov. 17, 2016) and can be found here: https://www.federalregister.gov/documents/2016/11/17/2016-27702/privacy-act-of-1974-publication-of-notices-of-systems-of-records-and-proposed-new-systems-of-records</p> <p>External Civil Rights Activities: No. OCR-EEO is working with IM-42 on a SORN (and records schedules) for its external civil rights enforcement activities.</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A</p>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>EEO Complaints Processing: DOE Federal employees who file an EEO complaint, individuals who are party to the EEO Complaint, witnesses, alleged responsible management officials, the Department, another Federal agency (e.g., EEOC, Merit Systems Protection Board), and EEO Investigators. In very limited circumstances, a DOE contractor may file an EEO complaint with the Department.</p> <p>External Civil Rights Activities: Any member of the public who files an external civil rights complaint with the Department, individuals or entities who are party to the external civil rights complaint, witnesses, participants in DOE external civil rights compliance reviews and other external civil rights compliance and enforcement activities, other Federal agencies, and DOE financial assistance recipients.</p>



MODULE II – PII SYSTEMS & PROJECTS

9. Will the information system derive new or meta data about an individual from the information collected?

EEO Complaints Processing: Individuals who file an EEO complaint with OCR-EEO will provide their name, contact information, and information relevant to the claim(s) they raise, especially the bases (e.g., age, race, etc.) and issues (e.g., suspension, removal, etc.). OCR-EEO will use that information to process the complaint through the administrative process, which includes but is not limited to: EEO counseling (which may result in a report detailing efforts to frame and/or resolve claims in the complaint); acceptance of claims for investigation; investigative report of those allegations, which will contain affidavits from witnesses and alleged responsible management officials, data about the complainant and complainant’s work unit, Departmental policies, and other documents relevant to the case (e.g., complainant’s performance rating, decision on request for reasonable accommodation, selection or non-selection for a position, etc.); dismissal of some or all allegations; a final decision on discrimination allegations, if requested or ordered; a settlement agreement resolving claims of discrimination and resolution terms; documents and information related to appeals of decisions to the U.S. Equal Employment Opportunity Commission and/or U.S. Merit System Protection Board; and documents related to civil actions filed in U.S. District Court.

External Civil Rights Activities: Regarding the complaints that OCR-EEO receives for our external civil rights legal authorities, the office will evaluate complaints (which will include names and contact information of complainants, including a description of the bases and issues in the claim(s)); generate correspondence to process complaints, including acceptance of claims and/or dismissals; possibly create investigative reports; possibly develop agreements with recipients of DOE FFA; and generate correspondence related to potential enforcement of these legal authorities with the U.S. Department of Justice and/or other Federal agencies. Regarding compliance reviews that OCR-EEO conducts of FFA recipients, the office may generate notifications and requests for information from FFA recipients; compliance reports; agreements with FFA recipients; correspondence regarding monitoring of such agreements; and other related correspondence. Compliance reviews may also result in the collection of information related to program participants or beneficiaries of DOE FFA. OCR-EEO may also generate similar correspondence regarding pre-award reviews of FFA awards.

For both program areas (EEO Complaints Processing and External Civil Rights Activities), the system will enable OCR-EEO to collect data and aggregate it into reports or other formats.



MODULE II – PII SYSTEMS & PROJECTS

<p>10. Are the data elements described in detail and documented?</p>	<p>Modules for both program areas are still in development. We can provide a copy of the EEOC Form 462 Guide that describes the data gathering requirements for the EEO Complaint Processing module. Our regulations at 10 CFR 1040, 1041, and 1042 can provide guidance on the types of data we are seeking to gather for our external civil rights enforcement activities.</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>EEO Complaints Processing: The information will be used to process, manage, and track EEO complaint activity for DOE. EEO complaint activity reports that are published publicly (e.g., 462 Report or No FEAR Act Report data) will not contain PII. Only reports utilized by those with a need to know will contain PII.</p> <p>External Civil Rights Activities: The information will be used to process, manage, and track external civil rights enforcement activities, including but not limited to complaints, investigations, compliance reviews, pre-award reviews, and technical assistance. External civil rights activity reports that are published publicly will not contain PII. Only reports utilized by those with a need to know will contain PII.</p>
<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>Please see the response to #9.</p>



MODULE II – PII SYSTEMS & PROJECTS

EEO Complaints Processing:

PII is only disseminated within the framework of administrative complaint processes and/or related litigation in federal court. EEO case information may be shared with a complainant’s designated representative for the complaint. EEO case information may also be shared with staff in the Office of General Counsel who have a need to know in their representation of the Department related to an EEOC hearing or appeal, an MSPB hearing or appeal, or a filing in U.S. District Court. EEO case information may also be shared with EEOC and/or MSPB, in relation to a request for hearing or appeal by a complainant. EEO case information may also be shared with an alleged responsible management official or witness. PII may also be shared with a contact within Human Capital (HC) to the extent required to carry out personnel actions ordered as corrective action, or the agreed terms for settlement. Aggregated EEO complaint statistical data from the system (which does not contain PII) 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 EEOC Form 462 Report.

13. With what other agencies or entities will an individual’s information be shared?

External Civil Rights Activities: Records may be disclosed to the following entities:

To the Department of Justice or other Federal and State agencies when necessary to conduct an investigation, enforce DOE’s external civil rights regulations which implement nondiscrimination statutes, or assure proper coordination between Federal agencies;

To recipients of DOE financial assistance, contractors, or consultants when necessary to conduct an investigation or otherwise engage in compliance and enforcement efforts pursuant to DOE’s external civil rights regulations, which implement nondiscrimination statutes;

To persons named as alleged discriminating officials to allow such persons the opportunity to respond to the allegations of discrimination made against them during the course of the discrimination complaint process; and

To any potential source of information when necessary to obtain information relevant to an OCR-EEO investigation of a discrimination complaint or related compliance activity, but only to the extent necessary to inform the source of the purpose(s) of the request and to identify the type of information requested.

REPORTS



MODULE II – PII SYSTEMS & PROJECTS

<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>For both of the program areas, the system will be able to run custom and ad-hoc reports for the purposes of tracking types of cases and/or work products and for identifying any cases and/or work products with similar data points. These custom and/or ad-hoc reports with case identifiers are for internal use only and are not released to individuals outside of the OCR-EEO Community.</p>
<p>15. What will be the use of these reports?</p>	<p>These custom and ad-hoc reports will be used to track types of cases, to identify similar types or cases and/or work products, and to generally use the data collected to better manage and share information about work processes and results of decisions made about cases and/or work products to improve overall program quality and efficiency.</p>
<p>16. Who will have access to these reports?</p>	<p>Only authorized users for either program area will have access to data and reports from relevant modules, and no users outside of the OCR-EEO Community will have access to CMTS.</p>
<p>MONITORING</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>N/A.</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A</p>



MODULE II – PII SYSTEMS & PROJECTS

19. Are controls implemented to prevent unauthorized monitoring of individuals?

The system will be utilized for EEO case management and tracking and for the management and tracking of external civil rights compliance and enforcement activities. The system is not designed to monitor individuals, but to manage complaint activity that is filed by individuals and to manage external compliance and enforcement activities.

OCR-EEO's agreement with WingSwept contains the following provision:

(b) *Safeguarding requirements and procedures.* (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems.

Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

* * * * *

DATA MANAGEMENT & MAINTENANCE



MODULE II – PII SYSTEMS & PROJECTS

20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.

EEO Complaint Processing: When an individual completes the initial intake form for an EEO complaint, they are required to certify that the information provided is true and accurate to the best of their knowledge. If an individual files a formal EEO complaint, and OCR-EEO accepts issues for investigation, the complainant, witnesses, and alleged responsible management officials are asked to provide affidavits in which they must attest to the accurateness of the information contained in their respective affidavits. Following an EEO investigation, a copy of the case file and the report of investigation are provided to the complainant, and the complainant may inform OCR-EEO of any inaccurate information.

External Civil Rights Activities: Information related to the filing of an external civil rights complaint will be evaluated to determine if the Department has jurisdiction over the complaint. In making that determination, portions of the complaint will be evaluated for accuracy. If a complaint is accepted for investigation, the investigator assigned to the case will attempt to validate or confirm the accuracy of information through interviews, email communications, and comparison of policies, data, and documents. In relation to compliance review activities, the OCR-EEO staff assigned to a review will work to verify the accuracy of information based on responses to questionnaires and data and document requests.

21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?

EEO Complaint Processing: Deployment, training, and maintenance of CMTS for EEO complaints processing will be overseen by OCR-EEO. OCR-EEO will provide specific instructions on how to enter information into CMTS regarding each step of the EEO complaint process and will regularly review the system to ensure that information is being entered consistently and accurately.

External Civil Rights Activities: All external civil rights activities are performed by OCR-EEO staff. OCR-EEO will regularly review the system to ensure that information is being entered consistently and accurately.

RECORDS MANAGEMENT



MODULE II – PII SYSTEMS & PROJECTS

<p>22. Identify the record(s).</p>	<p>EEO Complaints Processing:</p> <p>Informal Complaints: Records of cases that are filed at the informal EEO complaint stage that do not result in the filing of a formal EEO complaint.</p> <p>Formal Complaints: Records generated in response to the filing of a formal EEO complaint with the Department, by the U.S. Equal Employment Opportunity Commission, U.S. Merit Systems Protection Board, or by a U.S. District Court. Includes records gathered in the preliminary informal process, complaints, various forms of evidence, reports of investigation that contain affidavits, data, and exhibits, withdrawal notices, copies of decisions, records of hearings and appeals, and related documents.</p> <p>External Civil Rights Activities: records relating to external civil rights complaints; records relating to compliance reviews of FFA recipients; records relating to enforcement of civil rights obligations, if necessary; records regarding pre-award reviews of FFA awards; records regarding technical assistance regarding civil rights obligations of FFA recipients; and other records related to external civil rights compliance and enforcement activities.</p>
<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p>EEO Complaints Processing: General Records Schedule 2.3, Employee Relations, Item 110, EEO Discrimination Complaint Files – Informal Process. Temporary. Destroy 3 years after resolution of case, but longer retention is authorized if required for business use.</p> <p>EEO Complaints Processing: General Records Schedule 2.3, Employee Relations, Item 111, EEO Discrimination Complaint Files – Formal Process. Temporary. Destroy 7 years after resolution of case, but longer retention is authorized if required for business use.</p> <p>External Civil Rights Enforcement: OCR-EEO is working with OIRM on records schedules for all of its external civil rights activities. Until they are approved by NARA, such records are required to be treated like permanent records.</p>
<p>24. Records Contact</p>	<p>Kathy Reid</p> <p>kathy.reid@emcbc.doe.gov</p> <p>(513) 246-0607</p>

ACCESS, SAFEGUARDS & SECURITY



25. What controls are in place to protect the data from unauthorized access, modification or use?

OCR-EEO's agreement with Wingswept contains the following provision:

(b) *Safeguarding requirements and procedures.* (1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems.

Requirements and procedures for basic safeguarding of covered contractor information systems shall

include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of

authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems. Identify information system users, processes acting on behalf of users, or devices.

(v) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vi) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(vii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(viii) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(ix) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(x) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xi) Identify, report, and correct information and information system



MODULE II – PII SYSTEMS & PROJECTS

	<p>flaws in a timely manner.</p> <p>(xii) Provide protection from malicious code at appropriate locations within organizational information systems.</p> <p>(xiii) Update malicious code protection mechanisms when new releases are available.</p> <p>(xiv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.</p> <p>(2) <i>Other requirements.</i> This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.</p>
<p>26. Who will have access to PII data?</p>	<p>EEO Complaints Processing: The roles we have in our legacy system are: Administrator; Case Manager; Counselor; Master Administrator; Super Processor; Ultimate; Super-Manager. Similar roles/permissions will be established in CMTS for the OCR-EEO Community.</p> <p>External Civil Rights Enforcement: OCR-EEO Leadership, Attorney-Advisors, other designated employees, and administrative staff will have access to PII data.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>27. How is access to PII data determined?</p>	<p>EEO Complaints Processing: CMTS Modules for EEO Complaints Processing will be accessible for authorized users within OCR-EEO and within the OCR-EEO Community (approved users within DOE and NNSA) based on role and need-to-know basis. The system provides a range of privileges established by the System Owner and include the visibility of data, read/write access, business rules, and administrator functions. Case information maintained within the system may also be shared with the Office of General Counsel, others with a need to know, and other federal agencies (EEOC, the Merit Systems Protection Board, and U.S. District Courts) as required for EEO case processing, but these entities do not have access to the CMTS system.</p> <p>External Civil Rights Enforcement: OCR-EEO Leadership, Attorney-Advisors, other designated employees, and administrative staff will have access to PII data. Individuals within the OCR-EEO Community who do not have these roles will have not access to data related to External Civil Rights Activities.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>CMTS is not interconnected, and it does not exchange information with any other systems.</p>
<p>29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?</p>	<p>N/A</p>
<p>30. Who is responsible for ensuring the authorized use of personal information?</p>	<p>OCR-EEO leaders, managers, and supervisors are responsible for ensuring that their subordinates utilize data maintained within CMTS for authorized purposes only.</p> <p>Federal staff assigned to roles in the CMTS system are required to take annual training related to the Privacy Act and are responsible for safeguarding PII in accordance with Privacy Act requirements.</p>

END OF MODULE II



SIGNATURE PAGE

	Signature	Date
System Owner	Patricia Zarate _____ (Print Name) _____ (Signature)	_____ _____
Local Privacy Act Officer & Acting Chief Privacy Officer	Brooke Dickson _____ (Print Name) _____ (Signature)	_____ _____