Homeland Security

DHS 4300A Sensitive Systems Handbook

Attachment S1

Managing CREs Containing SPII

Version 9.1

July 24, 2012

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
1.0	March 14, 2011	Initial release
1.0	July 24, 2011	Final
9.1	July 24, 2012	No changes

CONTENTS

1.0 INTRODUCTION

The Office of Management and Budget (OMB) issued Memorandum 07-16 (M-07-16), *Safeguarding against and Responding to the Breach of Personally Identifiable Information*, in response to incidents involving the theft of government equipment and mobile devices containing Sensitive Personally Identifiable Information (Sensitive PII) and resulting in the compromise or potential compromise of the data.[1] One of the goals of M-07-16 is to improve privacy and security protection through enhanced data tracking by requiring Federal agencies to log all computer-readable extracts (CREs) from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required.

The purpose of the DHS Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII (CRE Policy or Policy) is to provide direction to DHS offices, components, and personnel for creating and managing CREs that contain Sensitive PII. DHS components may develop their own implementing procedures on CREs provided they meet the minimum requirements set forth in this CRE Policy.

Section 7 below, entitled *CRE Procedures*, defines the procedures for managing both routine and ad hoc CREs from a risk perspective. The procedures included herein minimize the risk of sensitive information being breached through effective data tracking. Routine CREs are CREs that are created as part of an established data retrieval process whereas ad hoc CREs are performed in response to a specific need for information and have not otherwise been previously authorized by management. Ad hoc CREs therefore require additional documentation and validation under this Policy.

1.1 Scope

This Policy applies to:

a) All DHS personnel, including any employee, contractor, company, consultant, partner, detailee or Government agency that is performing a Federal function on behalf of DHS.

b) All CREs containing Sensitive PII that are extracted from DHS owned systems, <u>except for</u> CREs:

i) Created during litigation to comply with discovery obligations, court orders, subpoenas, settlement agreements, or other compulsory legal process;

[1] Although this guidance specifically refers to "sensitive personally identifiable information," readers should recognize that OMB M-07-16 refers to "sensitive information" and understand that all CREs containing <u>any</u> DHS sensitive information, including Sensitive PII, should be adequately protected.

ii) Created during the search for records in response to requests under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C. 552a); or

iii) Created in response to a Congressional, Inspector General (IG) or General Accounting Office (GAO) request.

1.2 Policy

DHS personnel may only create and use CREs for authorized official purposes.[2] CREs may be shared only as authorized by the Privacy Act of 1974, and other applicable Federal law and policy.[3] CREs must be appropriately secured during storage and transmission in accordance with the *Handbook for Safeguarding Sensitive PII at DHS*.[4] Managing CREs at the Department of Homeland Security must also comply with the following:

a) Systems that as part of routine business remove Sensitive PII in the form of a CRE, (e.g., routine system-to-system transmissions of data (routine CREs)) shall address associated risks in the source's security plan (SP).

b) Sensitive PII contained within a non-routine or ad hoc CRE (e.g. CREs not included within the boundaries of a source system's security plan) shall not be removed, physically or otherwise, from a DHS facility without written authorization from the Data Owner who is responsible for ensuring that the disclosure of the CRE data is lawful and in compliance with this and applicable DHS privacy and security policies.

c) All ad hoc CREs must be documented, tracked, and validated every 90 days after their creation to ensure either continued authorized use or that they have been appropriately destroyed or erased.

d) Ad hoc CREs shall be erased within ninety (90) days unless the information included in the extracts is required beyond the ninety (90) day period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.

Section 7 below, entitled *CRE Procedures,* describes the procedures for managing routine CREs as well as documenting and validating ad hoc CREs.

1.3 Authorities

a) DHS 4300A Sensitive System Policy Directive and Handbook

b) DHS Privacy Act Procedures (6 C.F.R §5.31)

c) Office of Management and Budget (OMB) Guidance, M-06-16

---

[2] CREs are necessary for certain processes however the use of CREs are not recommended and should be limited. Alternatively, role-based access to Sensitive PII should be used to the extent possible.

[3] DHS 4300A Sensitive System Policy, section 3.14 Personally Identifiable Information

[4] https://dhsonline.dhs.gov/portal/jhtml/community.jhtml?community=PRIV&index=0&id=2020480043

d) OMB Guidance, M-07-16

e) Privacy Act of 1974, as amended (5 U.S.C. 552a)

f) Homeland Security Act of 2002, as amended (6 U.S.C. 552)

1.4 Effective Date

This Policy becomes effective 90 days following the date of publication as indicated on the title page.

2.0 DEFINITIONS

a) Computer-Readable Extract (CRE)

Any Federal record or collection of records containing Sensitive PII that is retrieved from a DHS-owned database through a query, reporting tool, extract generation tool, or other means that is then saved into removable media[5] and/or a separate computer-readable device or application such as another database, a spreadsheet, or a text file.

b) Routine CRE

A CRE created as part of an established, normal and repeatable data retrieval process and that occurs in response to defined triggers or schedules. For the purposes of this Policy, a repeatable data retrieval process is defined as any management approved event for creating a CRE specifically allowed or covered by the source system's written security plan (SP)[6] (e.g., routine system-to-system transmissions of data), and

i) Conducted in the ordinary course of transacting agency business on a regular basis, but not necessarily on a specific interval; or

ii) Covered by an existing interconnectivity security agreement (ISAs) or information sharing and access agreement (ISAA), which includes memoranda of understanding (MOU), memoranda of agreement (MOA), letters of intent, or other agreement regarding the transfer of data.[7]

[5] Removable media is defined as hard drives, including desk top and laptop computers, floppy disks, compact discs (CDs), USB drives, memory cards, and any other media that may be read or copied electronically. All removable media shall be appropriately labeled according to the requirements in DHS 4300A Sensitive Systems Policy, Section 4.3.2 *Media Marking and Transport.*

[6] It is recommended that where transfers are system-to-system, the recipient system's SP also include language addressing the receipt of any CREs.

[7] Policies and Procedures for drafting MOUs or MOAs can be found in DHS Management Directive Number: 0450.1 http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0450%201_mou_moa.pdf

Examples of routine CREs:

- A CRE from an operational database to allow employees to Telework from home once a week using government-issued laptops. Written instructions are issued to all Teleworking employees on how to create, secure, and delete CREs.
- A weekly CRE consisting of the names, SSNs, enter-on-duty dates, and salaries of active agency employees from a Human Resources database onto a CD-ROM. The CRE is provided to the Office of Personnel Management, Workforce and Retirement Division, on a weekly basis pursuant to an interagency MOU. Pursuant to the MOU, the CD-ROM is retained only until the data is successfully uploaded then is destroyed.

c) Ad hoc CRE

Any CRE that is not a routine CRE. Ad hoc CREs are usually unplanned, one-time data retrieval events created in response to a specific need for information and not otherwise previously authorized by management or covered in the source system's security plan or by an established ISAA.[8]

Examples of ad hoc CREs:

- An ad hoc CRE that is shared on a one-time basis with another agency in support of that agency's law enforcement investigation. E.g., a CRE on individuals who entered the United States at a specific Port of Entry (POE) at a particular date and time is requested by the local police department to assist with the investigation of a crime that occurred near the POE.
- An ad hoc CRE from a production (i.e., live) database is needed so an employee, tasked with a special project, can analyze the data and issue a report.

d) Data Owner

The agency, program or office that has responsibility for and the authority to determine the allowable uses of the data sought as part of a routine or ad hoc CRE. With some systems the Data Owner may also be the Program Manager, Business Owner or System Owner.[9]

e) Personally Identifiable Information (PII)

Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

f) Requesting Entity

[8] It is recommended that an ISAA be entered into for any data extract that may reoccur.

[9] The position titles used in this section may differ component to component. The titles used are representative and can be changed to reflect the appropriate title of the position associated with the described responsibilities.

The agency, program, office, or organization making a request for DHS data in the form of a CRE. The Requesting Entity may be the component that owns the data, another component within DHS, another government agency, or a private sector entity.

g) Sensitive Personally Identifiable Information (Sensitive PII)

Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII, when maintained by DHS, are sensitive as stand-alone data elements. Examples of such Sensitive PII when maintained by DHS include:

- Social Security number (SSN);
- Alien registration number (A-Number);
- Biometric identifier; or
- Other data elements such as driver's license number, financial account number, citizenship or immigration status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive.

h) Security Plan (SP)

Provides a complete description of the information system, including purposes and functions, system boundaries, architecture, user groups, interconnections, hardware, software, encryption techniques, transmissions, and network configuration. The SP also provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements.

i) System Owner

Responsible for the successful operation of the IT systems within their program area and are ultimately accountable for the security of the IT systems and programs under their control. System Owners ensure that appropriate administrative, technical, and physical safeguards are employed and practiced and determine to what extent the system Certification and Accreditation and SP permits data extracts.

3.0 CRE PROCEDURES

a) General CRE Policy

i) Regardless whether the CRE is routine or ad hoc, DHS personnel shall only create and use CREs for authorized official purposes. CREs may be shared only when permissible under the Privacy Act of 1974, and other applicable Federal law and policy. CREs must also be appropriately secured during storage and transmission in accordance with the Handbook for Safeguarding SPII at DHS.

b) Routine CREs

Routine CREs generally do not pose as great a privacy risk as ad hoc CREs because internal policies and procedures already exist that ensure CREs will be accounted for, appropriately secured, and erased/destroyed when no longer needed. Accordingly, this Policy does not require

routine CREs to be documented and validated every 90 days. However, they must be documented in the SP. The Chief Information Security Officer and Information System Security Officer, as owners of the SP, are responsible for validating with the Data Owner that all extracts meeting the definition of routine CRE[10] are accurately identified in the source's SP. Data Owners shall ensure that routine CREs are carried out with appropriate oversight, security, and diligence to ensure that Sensitive PII is protected and that CREs are used and destroyed in accordance with established policies and procedures.

Routine CRE – Example 1:

A DHS office permits CREs from its operational database that contains Sensitive PII. CREs are created to allow employees to Telework from home once a week using government-issued laptops. The DHS Office issues written instructions to all Teleworking employees on how to create, secure, and delete CREs. The instructions are attached to each employee's Telework agreement and reviewed with the employee by his/her supervisor before Telework can begin. The instructions require employees to:

- Create CREs containing the minimum sensitive data necessary to accomplish your work.
- Transport CREs directly from the office to your home, utilizing the securest method possible, such as a FIPS 140-2 validated encrypted government laptop, thumb drive or CD-ROM.
- To better track their location, segregate all CREs in a central folder on your laptop and erase when no longer needed.
- Once a CRE is no longer needed, erase it from your laptop or thumb drive, or destroy the CD-ROM using an approved government shredder.

This describes a routine CRE because the creation of the CRE occurs as part of an established data retrieval process (i.e., permitting the routine teleworking of agency employees) and the office has adequate procedures in place to ensure that CREs are properly secured then destroyed when no longer needed. The procedures mitigate the risk and provide protection for the Sensitive PII.

Routine CRE – Example 2:

Human Resources (HR) produces a weekly CRE consisting of the names, SSNs, enter-on-duty dates, and salaries of active agency employees. The CRE is provided to the Office of Personnel Management, Workforce and Retirement Division, on a weekly basis pursuant to an interagency MOU. HR tracks the CRE by entering it into a data extract log each week. The CRE is imported into an Excel spreadsheet then saved in secure encrypted format to a CD-ROM. HR delivers the CD-ROM to OPM using an agency-approved courier service. Pursuant to the MOU, OPM retains the CD-ROM until the data is successfully uploaded to its database, at which time they destroy the CD-ROM by shredding.

This describes a routine CRE because the creation of the CRE occurs as part of an established data retrieval process (i.e., to carry out an interagency MOU in support of personnel management functions) and the MOU provides for procedures to ensure the secure transmission of the data between agencies. Also, it requires the recipient to destroy the CRE once it has been successfully uploaded. HR has taken the additional step of tracking the CREs in a log which is a sound practice although not required for routine CREs under this guidance.

[10] See Section 6 for the definition of "routine CRE."

c) Ad hoc CREs

i) Ad hoc CREs generally pose a greater risk to security and privacy than routine CREs because of the lack of agreements or standardized practices to ensure the CREs are accounted for, appropriately secured, and destroyed when no longer needed. Therefore, this Policy imposes additional requirements on ad hoc CREs to better ensure that the Sensitive PII in the CRE is not lost or compromised.

ii) The following five steps will be followed for all ad hoc CREs:

(1) Request and Approval – Any request for an ad hoc CRE will be approved by the Data Owner, who will ensure the creation and disclosure of the CRE is consistent with controlling law and policy.

(a) When the Requesting Entity determines that an ad hoc CRE needs to be processed, the Requesting Entity will contact the Data Owner and provide a justification for the ad hoc CRE. The justification will include; name, organization, and contact information of the Requesting Entity, proposed ad hoc CRE use, and proposed period of ad hoc CRE use.

(b) The Data Owner will evaluate the ad hoc CRE request against all relevant and controlling law and/or policy, including but not limited to: the Privacy Act of 1974, the System of Records Notice (SORN) covering the collection, and any relevant Standard Operating Procedures (SOP) and/or data use policies to determine whether the request can be approved. The Data Owner will consult with the component Privacy Officer and/or legal counsel for guidance where appropriate.

NOTE: In some situations, a Requesting Entity may also be the Data Owner. In the event of such an internal request, the Data Owner will comply with all procedures for approving and validating an ad hoc CRE.

(2) Creation and Transmission – Approved ad hoc CREs will be created and transmitted using appropriate security controls to mitigate risk.

(a) If the Data Owner approves the ad hoc CRE, the Data Owner will coordinate with the System Owner to determine the best method of data extraction and transfer.

(b) The System Owner, in consultation with the system Information System Security Officer (ISSO),[11] will identify the appropriate security controls necessary to protect the ad hoc CRE. The System Owner will use the guidance in OMB-M-06-16 to identify the minimum set of controls necessary based on data sensitivity or classification of the data.[12]

[11] The system ISSO is responsible for ensuring the implementation and effectiveness of security controls in accordance with DHS policies.

[12] OMB M-06-16 requirements for protecting Privacy Sensitive Systems that permit removal of sensitive information outside of internal agency controls can be found in Appendix S to DHS 4300A Sensitive System Policy Handbook.

(3) Documentation – The Data Owner will maintain a record of the creation and transmission of all ad hoc CREs. It is strongly recommended that the Data Owner use a standardized Request and Approval Form to document and track all ad hoc CREs. A sample Request and Approval Form is attached as *Appendix A*. In addition, a sample CRE Tracking Tool is attached as *Appendix B.*

NOTE: Organizations may wish to track the CRE using only the Request and Approval Form in *Appendix A* or track the CRE separately via a database application set up similar to *Appendix B.*

(a) The Data Owner will communicate the approval to the Requesting Entity and, prior to transmitting the ad hoc CRE, will receive a written acknowledgement that the Requesting Entity will comply with the terms of the approval. Sample agreement language is attached as *Appendix C.*

(b) Upon transmitting the ad hoc CRE, the Data Owner will complete the information in the Request and Approval Form with the following information: any modification(s) to the original request, CRE handling instructions (e.g., email, courier, FedEx), and security measures (e.g., Products using Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2, NSA Type 2 or Type 1 encryption[13]), the CRE validation cycle, the data destruction options, and any waiver requests.

(c) The Data Owner is responsible for maintaining each CRE Request and Approval Form according to the applicable program or system records retention schedule. [14] The Request and Approval Form will document the Data Owner's compliance with these procedures, and may be audited during CRE compliance audits conducted by the DHS Privacy Office or the DHS Inspector General.

(4) Validation – Authorized ad hoc CREs can be used by the Requesting Entity for up to 90 days. After 90 days, the Data Owner will either re-authorize the ad hoc CRE for an additional period (not to exceed 90 days), or will confirm that the CRE has been destroyed.

(a) The Data Owner can re-authorize an ad hoc CRE multiple times, but an authorization can not exceed 90 days.

(b) The Data Owner will decide to authorize a Requesting Entity's request to retain a CRE for more than 90 days based upon the merit of the request.

(c) All validation (re-authorization) dates will be recorded on the Request and Approval Form.

---

http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/DHS%20Sensitive%20Systems%20Policy%204300A.doc

[13] DHS 4300A Sensitive System Policy, Section 5.5.1 *Encryption*.

[14] In the absence of an established retention schedule the Data Owner should plan to retain the Request and Approval Form for a minimum of 3 years after the ad hoc CRE is destroyed. The program or system's record retention schedule should be updated to reflect this new requirement.

(5) Destruction – ad hoc CREs will be destroyed timely, or as soon as they are no longer needed or when requested by the Data Owner.

(a) The method of destruction will comply with NIST Special Publication 800-88, *Guidelines for Media Sanitation*, and DHS standards detailed in *DHS 4300A, Sensitive System Policy*, section 4.3.3; *Media Sanitation and Disposal*.[15]

(b) Upon CRE destruction, the Data Owner will update the Request and Approval Form.

(c) If the Requesting Entity does not comply with destroying or confirming destruction of the ad hoc CRE, the Data Owner will report the situation as a privacy incident through the DHS privacy incident reporting process as outlined in the *DHS Privacy Incident Handling Guidance, v2.1*.[16]

(d) The CRE process is complete after the CRE destruction is noted in the Request and Approval Form. Until the CRE is destroyed, step 4 (validation) will continue to occur every 90 days.

(e) It is strongly recommended that the Data Owner obtain an attestation from the Requesting Entity regarding the destruction of the CRE. Sample CRE destruction attestation language is provided in *Appendix D.*

Ad-Hoc CRE – Example 1:

Division 1 needs to track that all of its undercover law enforcement employees complete mandatory annual training. Division 1 proposes to extract data from the DHS human resources (HR) database containing the first name, middle initial and last name of all Division 1 undercover law enforcement employees. Division 1 loads the extracted data into an Excel spreadsheet, which is used to track the dates that Division 1 employees completed annual training. This Excel tracking sheet is incorporated into Division 1's personnel records system.

In this scenario, Division 1 is the Requesting Entity and the DHS HR office is the Data Owner. Both parties need to go through all five steps of the ad hoc CRE process above. The data is considered Sensitive PII due to the sensitive nature of the individuals and their roles as undercover law enforcement employees.

Step 1: Request and Approval. The Division 1 supervisor contacts the HR office to request the ad hoc CRE. The HR office ensures that providing this information to Division 1 for this purpose is lawful and in accordance with relevant policies on privacy, seeking the help of the component privacy officer or legal counsel as needed. The HR official approves the request and informs Division 1 that the extract will be created. The HR official tells Division 1 they must destroy the CRE as soon as the new spreadsheet has been created.

Step 2: Creation and Transmission. The HR official determines how the extract needs to be transmitted to Division 1. In this case, it was decided that a CD-ROM is the simplest way to transmit the data to Division 1. The HR official creates the extract file in Excel, encrypts the file, and stores it on a CD-ROM and hand delivers it to Division 1.

Step 3: Documentation. The HR official, as the Data Owner, completes the Request and Approval

[15] http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/DHS%20Sensitive%20Systems%20Policy%204300A.doc

[16] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

Form and includes all the relevant information as required by this guidance.

Step 4: Validation. The HR official authorizes the ad hoc CRE for no more than 90 days. The agreed-upon length of time is recorded in the Request and Approval Form and adhered to.

In this example, the Data Owner does not have to contact the Requesting Entity for the usual 90-day validation because the CRE is likely destroyed before 90 days has passed. See Step 5 below.

Step 5: Destruction. Division 1 destroys the CD-ROM with the assistance of its Information System Security Officer (ISSO) using an approved method for destroying media. Division 1 notifies HR that the CD-ROM has been destroyed and HR makes a note of this in the Request and Approval Form.

The CRE process is complete because the CRE was destroyed and documented in the Request and Approval Form.

Ad-Hoc CRE – Example 2:

An employee is tasked with a one-time special project to analyze data maintained on a database server. Because working directly on production data is not possible, the employee requires an extract of the data be created and stored as an Excel spreadsheet on her local drive.

In this example, the employee is the Requesting Entity and the Data Owner is the business entity responsible for the database. Both parties need to go through the five steps outlined above and follow all procedures for managing ad hoc CREs to ensure compliance with DHS policy, and to document the creation and destruction of the CRE.

Step 1: Request and Approval. The employee requests permission from the Data Owner to extract Sensitive PII onto her hard drive. The Data Owner validates that the extract is in compliance with relevant policies, seeking the help of the component privacy officer or legal counsel as needed. The Data Owner directs the employee to destroy the data extract no later than 90 days after it is created or upon completion of the project, whichever is sooner. The System Owner will update the Request and Approval Form as necessary to indicate any additional 90 day time periods.

Step 2: Creation and Transmission. Following approval from the Data Owner the employee creates the extract and saves the data into the hard drive.

Step 3: Documentation. The employee ensures the Request and Approval Form is complete and includes all the relevant information as required by this guidance including the approval of the Data Owner in step 1.

Step 4: Validation. At the end of 90 days the Data Owner discusses with requestor and determines if the ad hoc CRE should be authorized for an additional 90 day period. The length of time should be recorded in the Request and Approval Form and adhered to. Each subsequent 90 day validation is recorded in the Request and Approval Form until the data use is no longer needed.

Step 5: Destruction. Upon completion of the project the employee will destroy the CRE and communicate the destruction status of the CRE to the Data Owner. The Data Owner documents the destruction of the data in the Request and Approval Form.

The CRE process is complete when the CRE is destroyed and its destruction documented in the Request and Approval Form.

APPENDIX S1 – COMPUTER-READABLE EXTRACT (CRE) SAMPLE REQUEST AND APPROVAL FORM

Computer-Readable Extract (CRE) Request & Approval	SUBMISSION DATE (mm/dd/yyyy)	APPROVED DATE (mm/dd/yyyy)	CREATION DATE (mm/dd/yyyy)

TO BE COMPLETED BY REQUESTING ENTITY

REQUESTING ENTITY CONTACT INFORMATION

Name	Title	Organization	E-mail	Telephone

CRE INFORMATION

Source System (SS)	System Owner	Organization	Data Requested	Range of Data (e.g. Data from AA to ZZ)
Recipient System	System Owner	Organization	Date CRE Required (Begin)	Date CRE Required (End)

REQUEST DESCRIPTION/JUSTIFICATION (Provide detailed requirements for CRE including how CRE will be used in Requesting Entity environment.)

CRE USERS (Provide a description of who will have access to the data. To the extent possible include; persons names, organizations and physical locations.)

CRE TRANSMISSION (Provide a description for how the data will be transported (ftp, disk, etc.) and to where it is being transported.)

WAIVER REQUEST and RATIONAL (Provide a detailed explanation for the waiver request below. Include which requirement(s) need to be waived as well as

TO BE COMPLETED BY DATA OWNER

DATA OWNER CONTACT INFORMATION

Name	Title	Organization	Email	Telephone

General CRE Type	CRE incorporated into Requesting Entity existing System of Record (SOR)?	CRE remain w/in SS Security Plan (SP) Boundary?
☐ Regular Business Activity ☐ One-time Request	☐ Yes SOR _____ ☐ No	☐ Yes ☐ No

MODIFICATION(S) TO ORIGINAL REQUEST (Identify any clarifications or modifications to original request including any restrictions on CRE use.)

HANDLING INSTRUCTIONS (Identify any specific controls Requesting Entity must implement to protect CRE.)

CRE VALIDATION CYCLE			DATA DESTRUCTION OPTION	
Period:*	1st Cycle	2nd Cycle 3rd Cycle	☐ Return CRE to Data Owner	Date Complete _____
	_____	_____ _____	☐ Requestor Destroy CRE (Attach fully executed attestation letter)	Date Complete _____
* Not to exceed 90 days				

CRE DECISION (Provide a detailed explanation for approving or denying the CRE request below.)

☐ Approved ☐ Rejected

Explanation:

WAIVER REVIEW and RATIONALE (Provide a detailed explanation for approving or denying the waiver request below.)

Decision on Waiver Request:

☐ Approved ☐ Rejected

Explanation:

DATA OWNER SIGNATURE

Signature:	Name:	Title:	Date:

APPENDIX S2 - COMPUTER-READABLE EXTRACT (CRE) SAMPLE TRACKING TOOL [17]

The Tracking Tool creates responsibility and accountability for ad hoc CREs with Sensitive PII by requiring the following information to be documented:

- Control Number - The number used to identify the data extract, if applicable
- Submission Date - The date the request was submitted (mm/dd/yyyy)
- Approved Date - The date the Data Owner approved the request (mm/dd/yyyy)
- Creation Date - The date the CRE was created (mm/dd/yyyy)
- Requesting Entity - Name of the entity (for agencies, include office or program name) receiving the CRE. Include contact information for an individual who will serve as the point-of-contact in that office or program
- Data Owner - First and last name of approving official, including agency name and contact information.
- Description - Describe the Sensitive PII being sent including purpose and justification for the request, e.g. 2,000 fingerprint pairs from XYZ database needed to respond to ABC agency request
- CRE Transmission - The media that is being used to transport or transfer the data from the secure system
- Purpose - The justification and description for the use of the data
- Encryption - Describe the use and/or level of encryption used to protect the Sensitive PII on the data extract
- Validation Date - Expiration date the Data Owner authorized for the ad hoc CRE. Not to exceed 90 days
- Final Disposition - Confirmation of destruction (include date), permanent transfer, or archival of data extract by appropriate official
- Comment - Any additional information necessary to facilitate tracking of the data extract

Control Number	Submission Date	Approved Date	Creation Date	Requesting Entity	Data Owner	Description	CRE Transmission	Purpose	Encryption Y/N	Validation Date(s)	Final Disposition	Comment

[17] This sample Request and Tracking Tool is derived from Appendix S2 – *Sample PII Tracking Log* of Attachment S to 4300A Sensitive System Policy Handbook. Please note that some of the categories and descriptions have changed based on the documenting and validating requirements contained in this policy.

APPENDIX S3 - COMPUTER-READABLE EXTRACT (CRE) SAMPLE DATA ACCESS AND USE AGREEMENT

1. **CONSTRAINTS ON DATA ACCESS AND USE**. The Parties agree to use and disclose the information exchanged between the Parties in a manner consistent with the requirements identified below and any other applicable routine uses, use restrictions or conditions imposed by law, including privacy compliance requirements stated in the Parties' applicable Privacy Impact Assessments (PIAs) and Privacy Act System of Records Notices (SORNs).

   A. Limitations on Access to Data.

   i. Requesting Entity will limit access to CRE records and data provided by Data Owner to only those Requesting Entity personnel who have a need-to-know the information to perform their duties.

   ii. Requesting Entity will ensure that all of its personnel with access to CRE records and data have been trained in the handling and sharing of such data including privacy training on the handling of PII. Recipient will ensure that all of its personnel with access to PII provided by Data Owner have been trained in the handling and sharing of such data, including privacy training on the handling of PII.

   B. Dissemination of Data:

   i. To the extent that Requesting Entity incorporates Data Owner records and data contained into a Privacy Act System of Records, Requesting Entity may share such information in accordance with the provisions of the Privacy Act of 1974, as amended (5 U.S.C. § 552a), including, as appropriate, sharing with Requesting Entity personnel who have an official need to know the information and sharing pursuant to the routine uses in the applicable SORN published by Requesting Entity.

   ii. Requesting Entity will not provide CRE records or data received to any commercial data provider. A commercial data provider is defined as a non-governmental entity that engages in the collection, aggregation, and sale of personal information. It does not include a government contractor hired to collect, maintain, analyze, and/or distribute records or data on the government's behalf.

   C. Sensitive Personally Identifiable Information (Sensitive PII): The Requesting Entity acknowledges that the CRE records and data provided to Requesting Entity is Sensitive PII and will be handled in accordance with DHS handling guidance for the same.

2. **SYSTEM SECURITY**. At a minimum the Requesting Entity shall safeguard the security, confidentiality, and integrity of the CRE and the systems on which the Sensitive PII data is stored, processed, and transmitted in accordance with the requirements established in the Handbook for Safeguarding Sensitive PII at the Department of Homeland Security. Additional conditions imposed by the Data Owner may be required and documented on the CRE Request & Approval form.

3. **DATA RETENTION**. The Requesting Entity may use the CRE for no more than 90 days. Data Owner will validate the on-going need for the CRE during that same time period.

4. **AUDITS**. Data Owner may audit the Requesting Entity's handling and maintenance of CRE to ensure compliance with any terms of the CRE approval. The audits will be conducted at the Data Owner's discretion and solely for the purpose of compliance. The Data Owner will be granted access to the Requesting Entity's systems and records deemed by the Data Owner to be necessary to conduct a complete audit of the handling of the CRE within 72 hours of a request by the Data Owner. The Data Owner may also accept the results of audits conducted by the Requesting Entity in lieu of a compliance audit.

APPENDIX S4 – COMPUTER-READABLE EXTRACT (CRE) SAMPLE DESTRUCTION ATTESTATION LANGUAGE

DHS Component: _____

DHS Data Owner: _____

Address: _____

_____

_____

By this letter, I am attesting to the destruction of the computer-readable extract described below.

I further attest that the below data extract was destroyed using agreed-upon destruction methodologies and/or methodologies consistent with the requirements contained within NIST Special Publication 800-88, *Guidelines for Media Sanitation* and DHS standards detailed in *DHS 4300A, Sensitive System Policy*, section 4.3.3; *Media Sanitation and Disposal*.

Description of Data Extract:

_____

_____

Destruction Method(s) Used:

_____

_____

Destruction Date:_____

Requesting Entity: _____

Representative: _____

Address: _____

_____

_____

_____/

Representative Signature / Date